Edge-corE NETWORKS | SMC Networks

USER GUIDE

BARRICADE™ N
802.11n Wireless 4-port Gigabit Broadband Router

SMCWGBR14-N2

Barricade™ N SMCWGBR14-N2 User Guide

SMC®
Networks
No. 1, Creation Road III,
Hsinchu Science Park,
30077, Taiwan, R.O.C.
TEL: +886 3 5770270
Fax: +886 3 5780764

September 2011
SMC-UG-0911-02

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice.

Copyright © 2011 by

SMC Networks, Inc.

No. 1 Creation Road III,
Hsinchu Science Park,
30077, Taiwan, R.O.C.

All rights reserved

Trademarks:

SMC is a registered trademark; and Barricade, EZ Switch, TigerStack, TigerSwitch, and TigerAccess are trademarks of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

Warranty and Product Registration

To register SMC products and to review the detailed warranty statement, please refer to the Support Section of the SMC Website at http://www.smc.com.

COMPLIANCES

FEDERAL COMMUNICATION COMMISSION INTERFERENCE STATEMENT

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

NOTE: The manufacturer is not responsible for any radio or tv interference caused by unauthorized modifications to this equipment. Such modifications could void the user’s authority to operate the equipment.

IMPORTANT NOTE:
FCC RADIATION EXPOSURE STATEMENT

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

CE MARK WARNING

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

NATIONAL RESTRICTIONS

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below.

Country	Restriction	Reason/Remark
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation	None	Only for indoor applications

NOTE: Do not use the product outdoors in France.

EUROPE - EU DECLARATION OF CONFORMITY

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- EN 60950-1:2006 + A11: 2009
  Safety of Information Technology Equipment.

- EN 300 328 V1.7.1: 2006-10
  Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive.

- EN 301 489-17 V1.8.1/ 2008-04
  EN 301 489-17 V2.1.1/ 2009-05
  Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2.4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment.

- EN 55022: 2006 + A1: 2007
  Limits and methods of measurement of radio disturbance characteristics of information technology equipment.

- EN 55024: 1998 + A1: 2001 + A2: 2003
  Information technology equipment immunity characteristics limits and methods of measurement.

- EN 62311: 2008
  Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz - 300 GHz).

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

This equipment may be operated in:

The official CE certificate of conformity can be downloaded by selecting the relevant model/ part number from www.smc.com -> support -> download.

Bulgarian Български	С настоящето, SMC Networks декларира, че това безжично устройство е в съответствие със съществените изисквания и другите приложими разпоредби на Директива 1999/5/ЕС.
Czech Česky	Manufacturer tímto prohlašuje, že tento Radio LAN device je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Danish Dansk	Undertegnede Manufacturer erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF
Dutch Nederlands	Hierbij verklaart Manufacturer dat het toestel Radio LAN device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG Bij deze Manufacturer dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
English	Hereby, Manufacturer, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Estonian Eesti	Käesolevaga kinnitab Manufacturer seadme Radio LAN device vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Finnish Suomi	Valmistaja Manufacturer vakuuttaa täten että Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
French Français	Par la présente Manufacturer déclare que l'appareil Radio LAN device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE
German Deutsch	Hiermit erklärt Manufacturer, dass sich dieser/diese/dieses Radio LAN device in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi) Hiermit erklärt Manufacturer die Übereinstimmung des Gerätes Radio LAN device mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
Greek Ελληνική	με την παρουσα Manufacturer δηλωνει οτι radio LAN device συμμορφωνεται προσ τισ ουσιωδεισ απαιτησεισ και τισ λοιπεσ σχετικεσ διαταξεισ τησ οδηγιασ 1999/5/εκ.
Hungarian Magyar	Alulírott, Manufacturer nyilatkozom, hogy a Radio LAN device megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Italian Italiano	Con la presente Manufacturer dichiara che questo Radio LAN device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latvian Latviski	Ar šo Manufacturer deklarē, ka Radio LAN device atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lithuanian Lietuvių	Šiuo Manufacturer deklaruoja, kad šis Radio LAN device atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Maltese Malti	Hawnhekk, Manufacturer, jiddikjara li dan Radio LAN device jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Polish Polski	Niniejszym Manufacturer oświadcza, że Radio LAN device jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Portuguese Português	Manufacturer declara que este Radio LAN device está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Romanian Română	SMC Networks declară că acest dispozitiv fără fir respectă cerințele esențiale precum şi alte dispoziții relevante ale Directivei 1999/5/EC.
Slovak Slovensky	Manufacturer týmto vyhlasuje, že Radio LAN device spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Slovenian Slovensko	Manufacturer izjavlja, da je ta radio LAN device v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Spanish Español	Por medio de la presente Manufacturer declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE
Swedish Svenska	Härmed intygar Manufacturer att denna Radio LAN device står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Turkish Turk	SMC Networks bu kablosuz cihazın temel gereksinimleri ve 1999/5/EC yonergesindeki ilgili koşulları karşıladığını beyan eder.

SAFETY PRECAUTIONS

Read the following information carefully before operating the device. Please follow the following precaution items to protect the device from risks and damage caused by fire and electric power:

- Use the power adapter that is included with the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburdened power outlet or damaged cords and plugs may cause electric shock or fire. Check the power cords regularly, if you find any damage, replace it at once.
- Proper space for heat dissipation is necessary to avoid any damage caused by device overheating. The ventilation holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these ventilation holes.
- Do not put this device close to a place where a heat source exits or high temperature occurs. Avoid placing the device in direct sunshine.
- Do not put this device close to a place which is damp or wet. Do not spill any fluid on this device.
- Please follow the instructions in the user manual/quick install guide carefully to connect the device to your PC or other electronic product. Any invalid connection may cause a power or fire risk.
- Do not place this device on an unstable surface or support.

PRÉCAUTIONS DE SÉCURITÉ

Lisez attentivement les informations suivantes avant d'utiliser votre appareil. Respectez toutes les précautions afin de protéger l'appareil des risques et dégâts provoqués par un incendie et l'alimentation électrique :

- Utilisez exclusivement l'adaptateur d'alimentation fourni avec cet appareil.
- Faites attention à la puissance de charge de la prise de courant ou des rallonges électriques. Une prise surchargée ou des cordons et des fiches endommagés peuvent provoquer une électrocution ou un incendie. Vérifiez régulièrement votre câble électrique. Si vous constatiez le moindre défaut, remplacez-le immédiatement.
- Il est primordial de laisser suffisamment d'espace autour de l'appareil pour permettre la dissipation de la chaleur et éviter les dégâts provoqués par une surchauffe de l'appareil. Les orifices de ventilation de l'appareil sont conçus pour permettre la dissipation thermique et garantir le bon fonctionnement de l'appareil. Ne couvrez jamais ces orifices.
- Ne placez pas cet appareil à proximité d'une source de chaleur ou dans un endroit exposé à des températures élevées. Evitez également de l'exposer à la lumière directe du soleil.
- Ne placez pas cet appareil à proximité d'un lieu humide ou mouillé. Prenez garde à ne renverser aucun liquide sur cet appareil.
- Merci de suivre les instructions du manuel d'utilisateur / guide d'installation rapide attentivement pour connecter l'appareil à votre PC ou à tout autre produit électronique. Toute connexion non valide peut provoquer un problème électrique ou un risque d'incendie.
- Ne placez pas cet appareil sur une surface ou un support instable.

SICHERHEITSMAßNAHMEN

Lesen Sie vor der Inbetriebnahme des Gerätes aufmerksam die nachstehenden Informationen. Bitte befolgen Sie die nachstehenden Sicherheitsmaßnahmen, damit das Gerät nicht beschädigt wird oder Gefahren durch Brand oder elektrische Energie entstehen:

- Verwenden Sie nur das beim Gerät mitgelieferte Netzteil.
- Achten Sie auf die Last der Steckdose oder des Verlängerungskabels. Eine überlastete Steckdose oder beschädigte Kabel und Stecker können Stromschläge und Brand verursachen. Prüfen Sie die Netzkabel regelmäßig. Ersetzen Sie sie umgehend, falls sie beschädigt sind.
- Achten Sie zur Vermeidung von Geräteschäden aufgrund von Überhitzung darauf, dass genügend Freiraum zur Wärmeabfuhr vorhanden ist. Die Belüftungsöffnungen am Gerät dienen der Wärmeabfuhr und damit der Gewährleistung eines normalen Gerätebetriebs. Decken Sie diese Belüftungsöffnungen nicht ab.

- Stellen Sie dieses Gerät nicht in der Nähe von Wärmequellen oder an Orten mit hohen Temperaturen auf. Platzieren Sie das Gerät nicht im direkten Sonnenlicht.

- Stellen Sie dieses Gerät nicht an feuchten oder nassen Orten auf. Achten Sie darauf, keine Flüssigkeiten über dem Gerät zu verschütten.

- Befolgen Sie die Hinweise im Benutzerhandbuch (bzw. in der Kurzanleitung) zum Anschluß des Gerätes an einen PC oder ein anderes Elektrogerät. Jegliche unzulässige Verbindung birgt die Gefahr von Stromschlägen und Brandgefahr.

- Platzieren Sie dieses Gerät nicht auf einer instabilen Oberfläche oder Halterung.

PRECAUCIONES DE SEGURIDAD

Lea la siguiente información detenidamente antes de utilizar el dispositivo. Siga las indicaciones de precaución que se mencionan a continuación para proteger el dispositivo contra riesgos y daños causados por el fuego y la energía eléctrica:

- Utilice el adaptador de alimentación incluido en el paquete del dispositivo.

- Preste atención a la carga de potencia de la toma de corriente o de los alargadores. Una toma de corriente sobrecargada o líneas y enchufes dañados pueden provocar descargas eléctricas o un incendio. Compruebe los cables de alimentación con cierta frecuencia. Si detecta algún daño, reemplácelos inmediatamente.

- Deje un espacio adecuado para que se disipe el calor y evitar así cualquier daño en el dispositivo causado por sobrecalentamiento. Los orificios de ventilación del dispositivo están diseñados para disipar el calor y garantizar que dicho dispositivo funciona con normalidad. No tape estos orificios de ventilación.

- No coloque este dispositivo cerca de un lugar donde haya una fuente de calor o temperaturas elevadas. Evite exponer el dispositivo a la luz solar directa.

- No coloque este dispositivo junto a un lugar húmedo o mojado. No derrame ningún fluido sobre el dispositivo.

- Por favor, siga cuidadosamente las instrucciones que figuran en el manual/guía de instalación rápida para conectar el dispositivo a su PC o a cualquier otro producto electrónico. Cualquier conexión no válida podría causar riesgo de descarga o de incendio.

- No coloque este dispositivo en una superficie o soporte inestable.

PRECAUÇÕES DE SEGURANÇA

Leia atentamente as seguintes informações antes de utilizar o dispositivo. Respeite as seguintes indicações de segurança para proteger o dispositivo contra riscos e danos causados por fogo e energia eléctrica:

- Utilize o transformador incluído na embalagem do dispositivo.
- Respeite a potência da tomada eléctrica e das extensões. Uma tomada eléctrica sobrecarregada ou cabos e fichas danificadas podem causar choques eléctricos ou fogo. Verifique regularmente os cabos de alimentação. Caso algum se encontre danificado, substitua-o imediatamente.
- É necessário deixar algum espaço livre em volta do dispositivo para dissipação de calor, de forma a evitar danos causados pelo sobreaquecimento do dispositivo. Os orifícios de ventilação do dispositivo foram concebidos para dissipar o calor e assegurar que o mesmo funciona normalmente. Não bloqueie esses orifícios de ventilação.
- Não coloque este dispositivo junto a fontes de calor ou em locais com temperaturas elevadas. Evite colocar o dispositivo sob luz solar directa.
- Não coloque este dispositivo junto a locais molhados ou com humidade. Não derrame líquidos sobre o dispositivo.
- Por favor siga atentamente as instruções do manual / guia de instalação rápida para conectar o dispositivo ao seu PC ou a qualquer outro dispositivo electrónico. Atenção que qualquer tipo de ligação inválida pode originar risco de choque eléctrico ou de incêndio.
- Não coloque este dispositivo numa superfície ou suporte instáveis.

About This Guide

Purpose

This guide details the hardware features of the wireless router, including its physical and performance-related characteristics, and how to install the device and use its configuration software.

Audience

This guide is for PC users with a working knowledge of computers. You should be familiar with Windows operating system concepts.

Conventions

The following conventions are used throughout this guide to show information:

Note: Emphasizes important information or calls your attention to related features or instructions.

Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Warning: Alerts you to a potential hazard that could cause personal injury.

Related Publications

The following publication gives basic information on how to install and use the wireless router.

Quick Installation Guide

Also, as part of the wireless router's software, there is online help that describes all configuration related features.

Revision History

This section summarizes the changes in each revision of this guide.

September 2011 Revision

This is the second revision of this guide. It includes the following change:

- Updated the Compliances section.

May 2011 Revision

This is the first revision of this guide.

CONTENTS

WARRANTY AND PRODUCT REGISTRATION 4

COMPLIANCES 5

ABOUT THIS GUIDE 13

CONTENTS 14

1 INTRODUCTION 17

Conventions 18

Main Features 18

Key Hardware Features 19

Package Contents 19

Front Panel 19

LED Indicators 20

Rear Panel 21

Antennas 21

Power Connector 21

Reset Button 21

USB Port 21

Ethernet WAN Port 22

Ethernet LAN Port 22

2 CONNECTING THE ROUTER 23

System Requirements 23

Installation Environment Requirements 23

Connecting the Router 24

3 QUICK INSTALLATION GUIDE 26

TCP/IP Configuration 26

Quick Installation Guide 28

4 CONFIGURING THE ROUTER 34

Login 34

Status 35

General Status 35
ARP List 35
Quick Setup 36

5 NETWORK SETTINGS 37
WAN 37
MAC Clone 46
LAN 47
Dynamic DNS 47
Comexe.cn DDNS 48
Dyndns.org DDNS 49
No-ip.com DDNS 50
Binding Setting 51

6 WIRELESS SETTINGS 53
Wireless Settings 53
Wireless Security 56
Wireless MAC Filtering 59
Wireless Advanced 61
Wireless Statistics 63
WPS 63

7 DHCP SETTINGS 72
DHCP Settings 72
DHCP Clients List 73
Address Reservation 74

8 USB STORAGE SETTINGS 76
Sharing Service 76
User Accounts 78

9 SPECIAL APPLICATION SETTINGS 80
Virtual Servers 80
Port Triggering 82
DMZ 84
UPnP 85

10 SECURITY SETTINGS 86
Basic Security 86
Advanced Security 88

11 ACCESS CONTROL SETTINGS 90

Rule 90

Host 93

Target 95

Schedule 97

Parental Control 99

12 ADVANCED ROUTING 103

Static Routing List 103

13 QOS SETTINGS 105

QoS Settings 105

Rules List 106

14 SYSTEM TOOLS 107

Time Setting 107

Diagnostic 108

Settings Management 110

Firmware Upgrade 110

Factory Defaults 111

Backup & Restore 111

Reboot 112

Password 113

System Log 114

Statistics 116

Local Management 117

Remote Management 118

A FAQ 120

B CONFIGURING THE PCS 125

C HARDWARE SPECIFICATIONS 128

GLOSSARY 130

1 INTRODUCTION

The SMCWGBR14-N2 Wireless N Gigabit Router integrates a 4-port switch, firewall, NAT router, and wireless access point. The Wireless N Gigabit Router delivers exceptional range and speed, which can fully meet the needs of Small Office/Home Office (SOHO) networks and users demanding higher networking performance.

INCREDIBLE SPEED

The SMCWGBR14-N2 Wireless N Gigabit Router provides wireless connections up to 300 Mbps with other 802.11n wireless clients. The incredible speed makes it ideal for handling multiple data streams at the same time, which ensures your network remains stable and smooth. The performance of this 802.11n wireless router gives you an unexpected networking experience at a speed 650% faster than 802.11g. It is also compatible with all IEEE 802.11g and IEEE 802.11b products.

MULTIPLE SECURITY PROTECTION

With multiple protection measures, including SSID broadcast control, 64/128/152-bit WEP encryption, Wi-Fi Protected Access (WPA2-PSK, WPA-PSK), as well as advanced firewall protection, the SMCWGBR14-N2 Wireless N Gigabit Router provides complete data privacy.

FLEXIBLE ACCESS CONTROL

The SMCWGBR14-N2 Wireless N Gigabit Router provides flexible access control, so that parents or network administrators can establish restricted access policies for children or staff. It also supports Virtual Server and DMZ host for Port Triggering, so that network administrators can manage and monitor the network in real time using remote management.

SIMPLE INSTALLATION

Since the SMCWGBR14-N2 is compatible with all major operating systems, it is very easy to manage. A Quick Setup Wizard is supported and detailed step-by-step instructions are provided in this user guide. Before installing the device, please read this guide to understand all the device’s functions.

CONVENTIONS

The "Router" or "SMCWGBR14-N2" mentioned in this guide stands for the SMCWGBR14-N2 Wireless N Gigabit Router without any explanation.

MAIN FEATURES

- Complies with IEEE 802.11n to provide a wireless data rate of up to 300 Mbps.
- One 10/100/1000 Mbps Auto-Negotiation RJ-45 WAN port, four 10/100/1000 Mbps Auto-Negotiation RJ-45 LAN ports, supporting Auto MDI/MDIX
- Provides WPA/WPA2, WPA-PSK/WPA2-PSK authentication, TKIP/AES encryption security.
- Shares data and Internet access for users, supporting Dynamic IP/Static IP/PPPoE Internet access.
- Supports multiple SSIDs, which allows different network access for wireless clients that is appropriate to their security or needs.
- Supports Virtual Server, Special Application and DMZ host.
- Supports UPnP, Dynamic DNS, Static Routing.
- Provides automatic and scheduled Internet connection.
- Built-in NAT and DHCP server supporting static IP address assignment.
- Supports Parental Control and Access Control.
- Supports PPPoE Internet-on-demand connection/disconnection
- Provides 64/128/152-bit WEP encryption security and wireless LAN ACL (Access Control List).
- Supports Flow Statistics.
- Supports firmware upgrade and Web management.

KEY HARDWARE FEATURES

The following table describes the main hardware features of the wireless Router.

Table 1: Key Hardware Features

Feature	Description
WAN Port	One 1000BASE-T RJ-45 port for connecting to the Internet.
LAN Port	Four 1000BASE-T RJ-45 ports for local network connections.
USB Port	One USB slot for USB mass storage device.
Reset Button	For resetting the unit and restoring factory defaults.
LEDs	Provides LED indicators for Power, WAN port, LAN port, and WLAN status.

PACKAGE CONTENTS

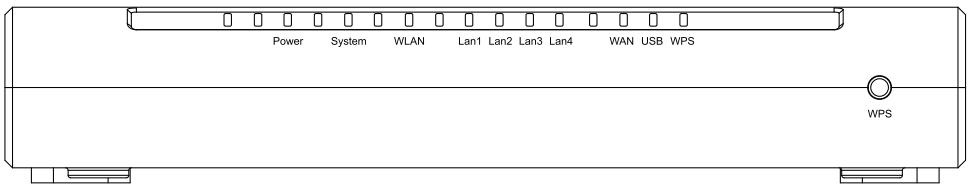
The Wireless N Gigabit Router package includes:

- SMCWGBR14-N2 Wireless N Gigabit Router
- DC power adapter
- Quick Installation Guide
- Resource CD for SMCWGBR14-N2 Wireless N Gigabit Router, including:
  - This User Guide
  - Other helpful information

Inform your dealer if there are any incorrect, missing or damaged parts. If possible, retain the carton, including the original packing materials. Use them again to repack the product in case there is a need to return it.

FRONT PANEL

Figure 1: Front Panel



LED INDICATORS

The wireless Router includes ten status LED indicators, as described in the following table.

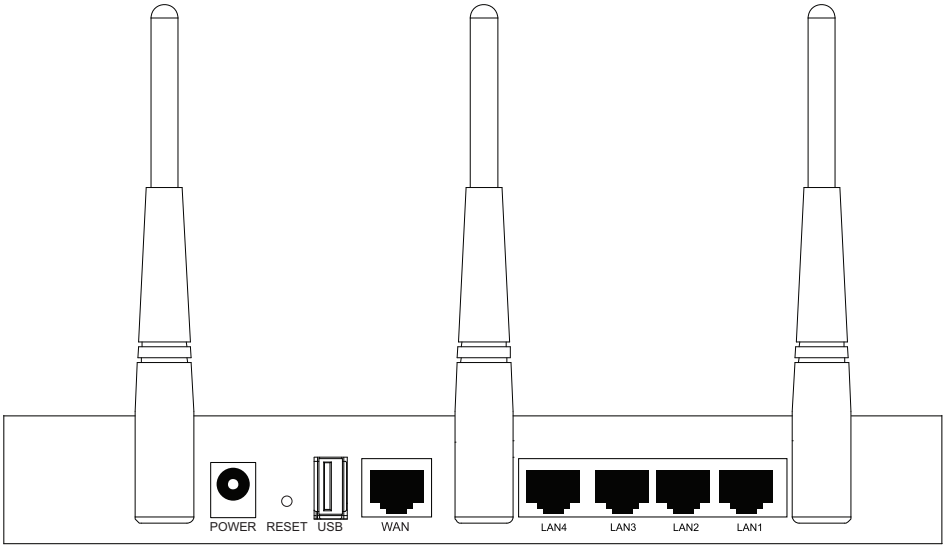
Table 2: LED Behavior

LED	Status	Description
Power	On	The unit is receiving power and is operating normally.
	Off	There is no power currently being supplied to the unit.
System	On	The Router is initializing.
	Flashing	The Router is working properly.
	Off	The Router has a system error.
WLAN	On/Flashing	The 802.11n radio is enabled and transmitting or receiving data through wireless links.
	Off	The 802.11n radio is disabled.
LAN (4 LEDs)	On	The Ethernet LAN port is connected to a PC or server.
	Flashing	The Ethernet port is connected and is transmitting or receiving data.
	Off	The Ethernet port is disconnected.
WAN	On	The port has a valid connection to another device.
	Flashing	The port is connected and is transmitting/receiving data.
	Off	The port is disconnected.
WPS	On	Indicates the WPS authentication of a device has been successfully completed.
	Fast Flashing	A wireless device failed to be added to the network by WPS.
	Slow Flashing	A wireless device is connecting to the network by WPS. This process will last for 2 minutes.
	Off	The WPS is not in progress.

NOTE: After a device is successfully added to the network by WPS, the WPS LED will remain on for about 5 minutes and then turn off.

REAR PANEL

Figure 2: Rear Panel



The following items are located on the rear panel (from left to right).

ANTENNAS The access point includes integrated MIMO antennas for wireless communications. A MIMO antenna system uses two or more identical antennas to receive and transmit signals, helping to increase data throughput and range. The antennas transmit the outgoing signal as a toroidal sphere (doughnut shaped), with the coverage extending most in a direction perpendicular to the antenna. The antennas should be adjusted to an angle that provides the appropriate coverage for the service area.

POWER CONNECTOR The wireless router must be powered with its supplied power adapter. Failure to do so results in voiding of any warrantly supplied with the product.

RESET BUTTON The Reset button is used to restore the factory default configuration. If you hold down the button for 5 seconds or more, any configuration changes you may have made are removed, and the factory default configuration is restored to the wireless router.

USB PORT Connects with a USB mass storage device.

ETHERNET WAN PORT

A 1000BASE-T RJ-45 port that can be attached to an Internet access device, such as a DSL or Cable modem.

ETHERNET LAN PORT

The wireless router has four 1000BASE-T RJ-45 ports that can be attached directly to a PC or 10BASE-T/100BASE-TX/1000BASE-T LAN segments.

This port supports automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs, switches, or hubs.

2 Connecting the Router

System Requirements

You must meet the following minimum requirements:

- Broadband Internet access service (DSL/Cable/Ethernet)
- One DSL/Cable modem that has an RJ-45 connector
- PCs with working Ethernet adapters and Ethernet cables with RJ-45 connectors
- TCP/IP protocol on each PC
- Web browser, such as Microsoft Internet Explorer 5.5 or above, Netscape Navigator 4.7 or above, or Mozilla Firefox 1.0 or above.

Installation Environment Requirements

- Place the Router in a well ventilated place far from any heater or heating vent
- Avoid direct irradiation from any strong light (such as sunlight)
- Keep at least 2 inches (5 cm) of clear space around the Router
- Operating Temperature: 0°C~40°C (32°F~104°F)
- Operating Humidity: 10%~90%RH, Non-condensing

CONNECTING THE ROUTER

Before installing the Router, make sure your PC is successfully connected to the Internet through the broadband service. If there is any problem, first contact your ISP.

Install the Router according to the following steps.

1. Power off your PC, Cable/DSL modem, and the Router.

2. Find a good location for the Router. The best place is usually at the center of your network. The location must meet the Installation Environment Requirements (page 23).

3. Adjust the position of the antennas. Normally, upright is the best position.

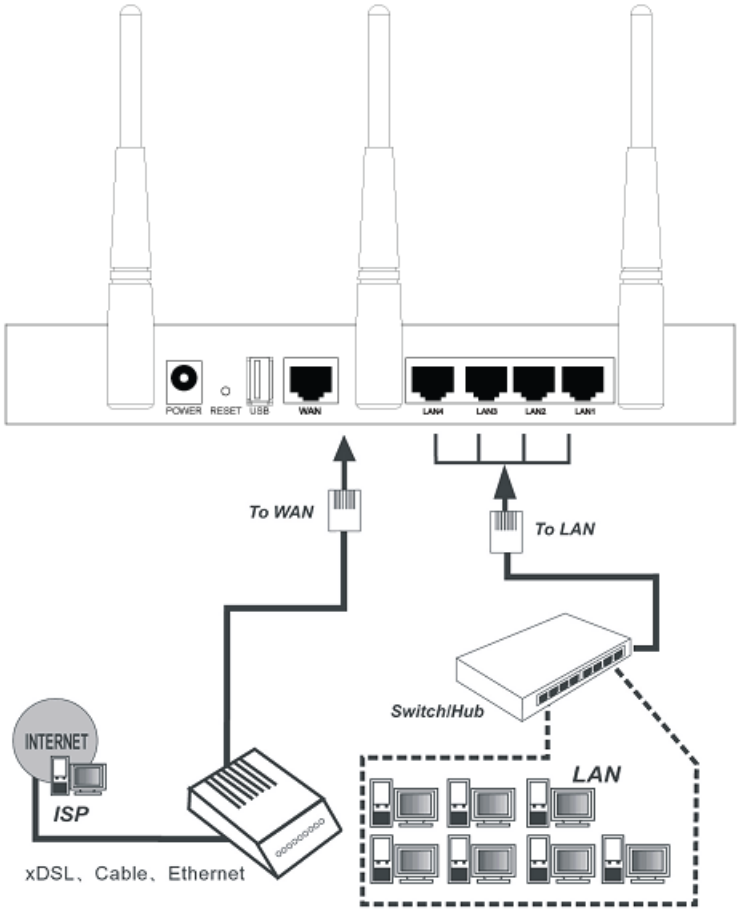
4. Connect wired PCs and switches/hubs to the LAN ports on the Router, as shown in Figure 3 on page 25.

5. Connect the DSL/Cable modem to the WAN port on the Router, as shown in Figure 3 on page 25.

6. Connect the power adapter to the power socket on the Router, and the other end into an electrical outlet. The Router will start to work automatically.

7. Power on your PC and Cable/DSL modem.

Figure 3: Hardware Installation



3 QUICK INSTALLATION GUIDE

TCP/IP CONFIGURATION

This chapter shows you how to quickly configure the basic functions of your SMCWGBR14-N2 Wireless N Gigabit Router using the Quick Setup Wizard.

The default IP address of the SMCWGBR14-N2 Wireless N Gigabit Router is 192.168.2.1. And the default Subnet Mask is 255.255.255.0. These values can be changed as needed. In this guide, the default values are used for all descriptions.

Connect a local PC to one of the LAN ports on the Router. Then configure the IP address for the PC in one of the following two ways.

Configure the IP address manually

1. Set up the TCP/IP Protocol for your PC. If you need instructions on how to do this, refer to "Configuring the PCs" on page 125.

2. Configure the network parameters. The IP address is 192.168.2.xxx ("xxx" is any number from 2 to 254), the Subnet Mask is 255.255.255.0, and the Gateway is 192.168.2.1 (the Router's default IP address).

Obtain an IP address automatically

1. Set the TCP/IP Protocol to "Obtain an IP address automatically" mode on your PC. If you need instructions on how to do this, refer to "Configuring the PCs" on page 125.

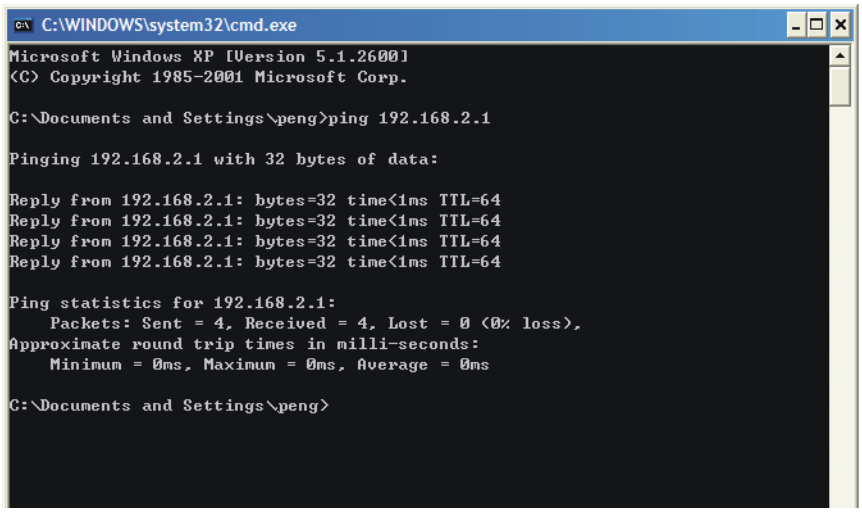
2. The built-in DHCP server will assign an IP address for the PC.

Now you can run the Ping command from the command prompt to verify the network connection between your PC and the Router. The following example is for Windows 2000 OS.

Open a command prompt, and type "ping 192.168.2.1" and then press Enter.

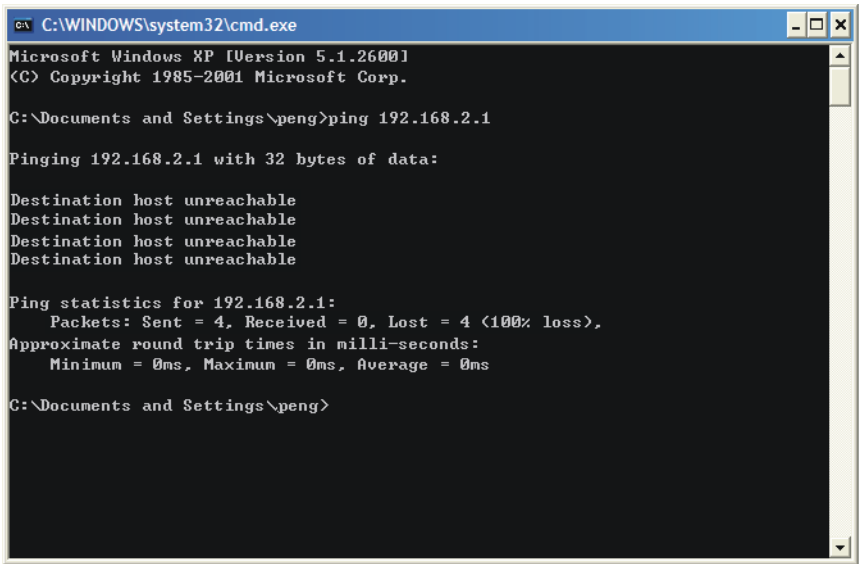
If the displayed result is similar to the following figure, it means the connection between your PC and the Router is functioning.

Figure 4: Success Result of a Ping Command


C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\peng>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Documents and Settings\peng>

If the displayed result is similar to the following figure, it means the connection between your PC and the Router is not functioning.

Figure 5: Failure of a Ping Command


C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\peng>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Destination host unreachable
Destination host unreachable
Destination host unreachable
Destination host unreachable
Ping statistics for 192.168.2.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Documents and Settings\peng>

To check the connection, follow these steps:

1. Verify that the LAN port LED to which the PC is connected on the Router and the LED on your PC's network adapter are turned on.

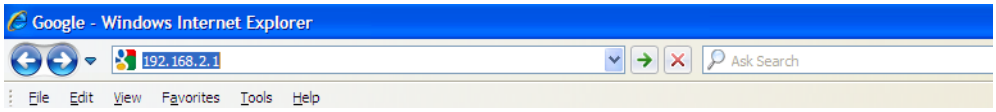
2. Verify that the Router's IP address is 192.168.2.1, and that your PC's IP address is within the range of 192.168.2.2 ~ 192.168.2.254.

QUICK INSTALLATION GUIDE

With a Web-based (Internet Explorer or Netscape® Navigator) utility, it is easy to configure and manage the SMCWGBR14-N2 Wireless N Gigabit Router. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser.

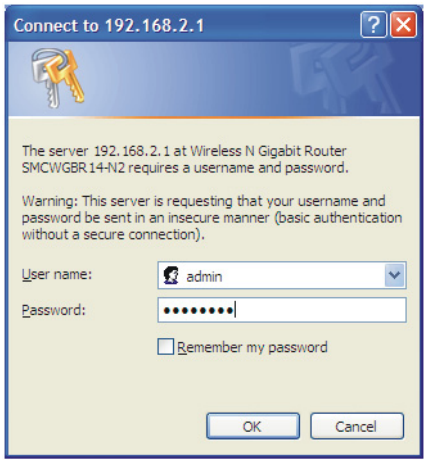
1. To access the configuration utility, open a web-browser and type the default address http://192.168.2.1 in the address field of the browser.

Figure 6: Log in to the Router



After a moment, a login window will appear. Enter "admin" for the User Name and "smcadmin" for the Password, both in lower case letters. Then click the OK button or press the Enter key.

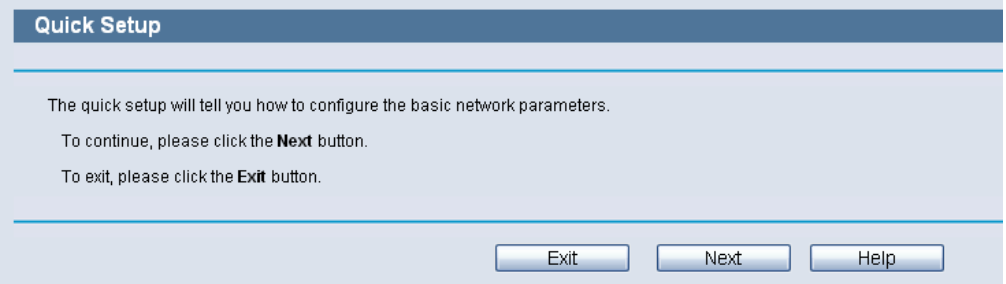
Figure 7: Login Windows


Connect to 192.168.2.1
The server 192.168.2.1 at Wireless N Gigabit Router SMCWGBR14-N2 requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

NOTE: If the above screen does not display, it means that your Web-browser has been set to a proxy. Go to Tools menu>Internet Options>Connections>LAN Settings, in the screen that appears, cancel the Using Proxy checkbox, and click OK to finish it.

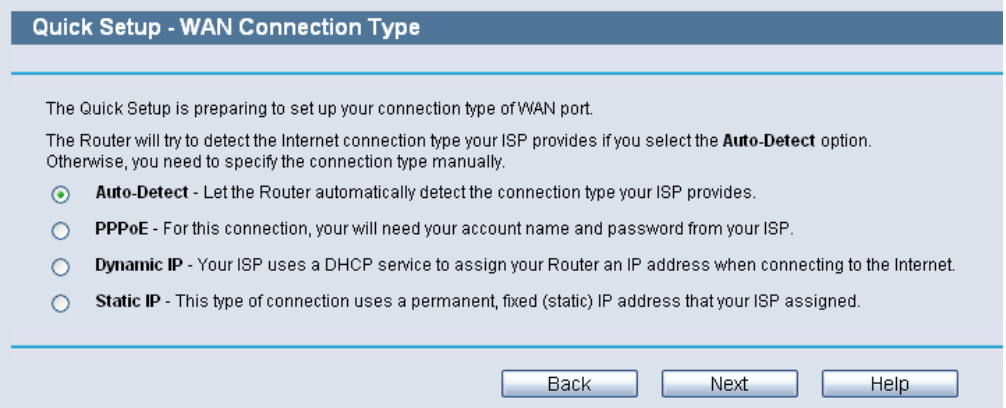
2. After successfully login, you can click the Quick Setup to quickly configure your Router.

Figure 8: Quick Setup


Quick Setup
The quick setup will tell you how to configure the basic network parameters.
To continue, please click the Next button.
To exit, please click the Exit button.
Exit
Next
Help

3. Click Next, and then WAN Connection Type page will appear.

Figure 9: Choose WAN Connection Type


Quick Setup - WAN Connection Type
The Quick Setup is preparing to set up your connection type of WAN port.
The Router will try to detect the Internet connection type your ISP provides if you select the Auto-Detect option. Otherwise, you need to specify the connection type manually.
Auto-Detect - Let the Router automatically detect the connection type your ISP provides.
PPPoE - For this connection, your will need your account name and password from your ISP.
Dynamic IP - Your ISP uses a DHCP service to assign your Router an IP address when connecting to the Internet.
Static IP - This type of connection uses a permanent, fixed (static) IP address that your ISP assigned.
Back
Next
Help

The Router provides Auto-Detect function and supports three popular ways PPPoE, Dynamic IP, and Static IP, to connect to the Internet. It is recommended that you make use of the Auto-Detect function. If you are sure of what kind of connection type your ISP provides, you can select the type and click Next to go on configuring.

4. If you select Auto-Detect, the Router will automatically detect the connection type your ISP provides. Make sure the cable is securely plugged into the WAN port before detection. The appropriate configuration page will be displayed when an active Internet service is successfully detected by the Router.

   a. If the connection type detected is PPPoE, the next screen will appear.

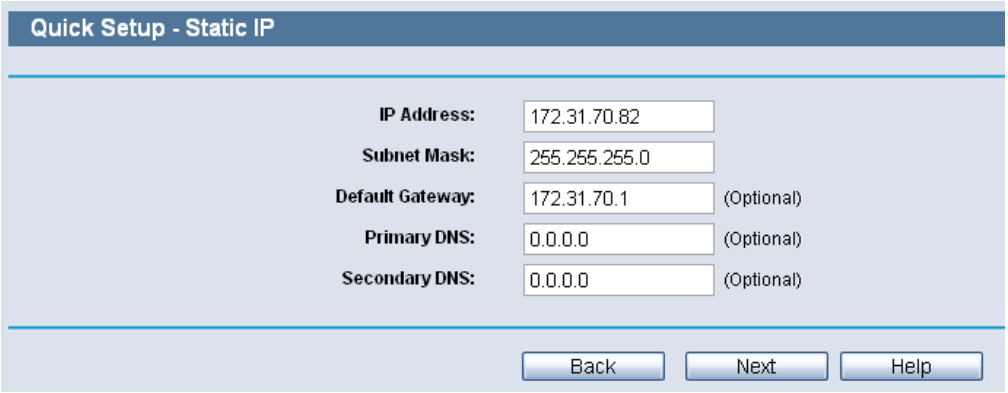
Figure 10: Quick Setup - PPPoE

- User Name and Password - Enter the User Name and Password provided by your ISP. These fields are case sensitive. If you have difficulty with this process, please contact your ISP.

b. If the connection type detected is Dynamic IP, you can go on with the wireless configuration, as shown in Figure 12 on page 31.

c. If the connection type detected is Static IP, the next screen will appear.

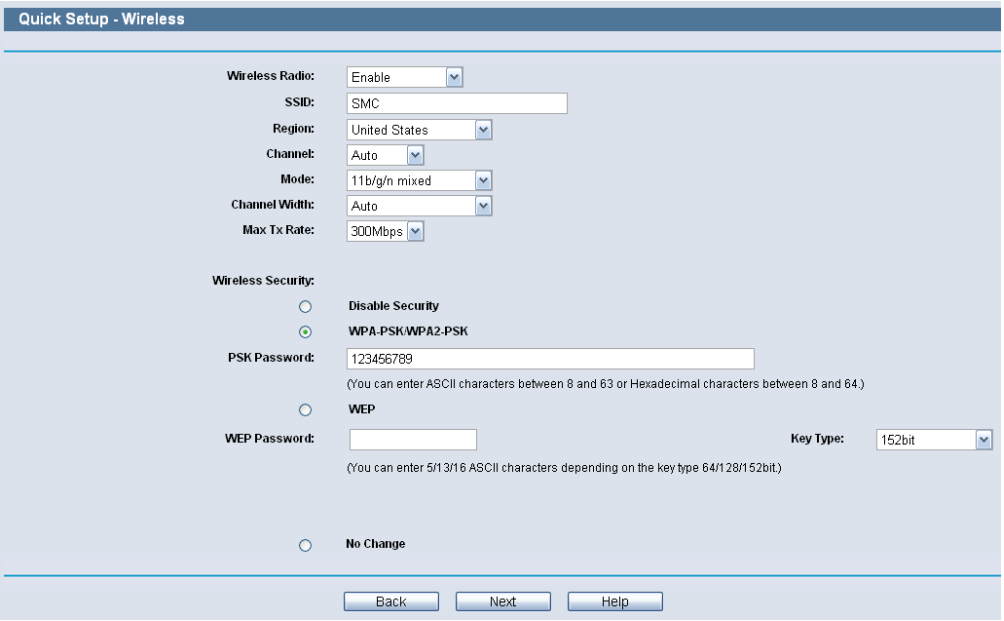
Figure 11: Quick Setup - Static IP



- IP Address - This is the WAN IP address as seen by external users on the Internet (including your ISP). Enter the IP address into the field.
- Subnet Mask - The Subnet Mask is used for the WAN IP address, it is usually 255.255.255.0.
- Default Gateway - Enter the gateway IP address into the box, if required.
- Primary DNS - Enter the DNS Server IP address into the box, if required.
- Secondary DNS - If your ISP provides another DNS server, enter it into this field.

5. Click Next to continue, the Wireless settings page will appear.

Figure 12: Quick Setup - Wireless



- **Wireless Radio** - Enable or disable the wireless radio choosing from the pull-down list.

- **SSID** - Enter a value of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security, the default SSID is set to be "SMC". This value is case-sensitive. For example, "TEST" is NOT the same as "test".

- **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the Router can be used. It may be illegal to use the wireless function of the Router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

- **Channel** - This field determines which operating frequency will be used. The default channel is set to Auto, so the AP will choose the best channel automatically. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

- **Mode** - This field determines the wireless mode which the Router works on.

- **Channel Width** - Select any channel width from the pull-down list. The default setting is automatic, which can adjust the channel width for your clients automatically.

- **Max Tx Rate** - You can limit the maximum transmission rate of the Router through this field.
- **Disable Security** - The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the Router without encryption. It is recommended strongly that you choose one of following options to enable security.
- **WPA-PSK/WPA2-PSK** - Select WPA based on pre-shared passphrase.
  - PSK Password - You can enter ASCII or Hexadecimal characters.

    For ASCII, the key can be made up of any numbers 0 to 9 and any letters A to Z, the length should be between 8 and 63 characters.

    For Hexadecimal, the key can be made up of any numbers 0 to 9 and letters A to F, the length should be between 8 and 64 characters.

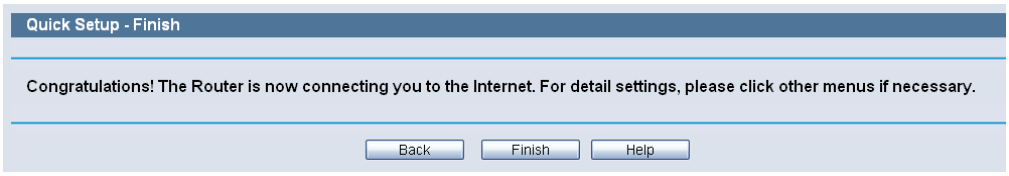
    Please also note the key is case sensitive, this means that upper and lower case keys will affect the outcome. It would also be a good idea to write down the key and all related wireless security settings.
- **No Change** - If you chose this option, wireless security configuration will not change!

These settings are only for basic wireless parameters. For advanced settings, please refer to "Wireless Settings" on page 53.

6. Click the Next button. You will then see the Finish page.

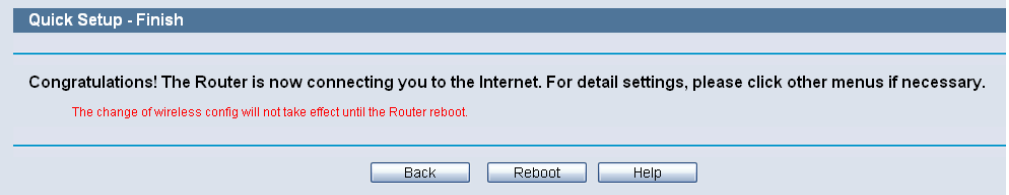
If you don't make any changes on the Wireless page, you will see the Finish page as below. Click the Finish button to finish the Quick Setup.

Figure 13: Quick Setup - Finish


Quick Setup - Finish
Congratulations! The Router is now connecting you to the Internet. For detail settings, please click other menus if necessary.
Back
Finish
Help

If there is something changed on the Wireless page, you will see the Finish page as in the following figure. Click the Reboot button to make your wireless configuration take effect and finish the Quick Setup.

Figure 14: Quick Setup - reboot


Quick Setup - Finish
Congratulations! The Router is now connecting you to the Internet. For detail settings, please click other menus if necessary.
The change of wireless config will not take effect until the Router reboot.
Back
Reboot
Help

4 CONFIGURING THE ROUTER

This chapter will show each Web page's key functions and the configuration method.

LOGIN

After your successful login, you will see the twelve main menus on the left of the Web-based utility. On the right, there are the corresponding explanations and instructions.

Figure 15: Main Menu

The detailed explanations for each Web page’s key function are listed below.

STATUS

GENERAL STATUS

The Status page provides the current status information about the Router. All information is read-only.

Figure 16: Router Status

ARP LIST

To manage the computer, you could observe the computers in the LAN by checking the relationship of MAC address and IP address on the ARP list, and you could configure the items on the ARP list also. This page displays the ARP List; it shows all the existing IP & MAC Binding entrie.

Figure 17: ARP List

- **MAC Address** - The MAC address of the controlled computer in the LAN.
- **IP Address** - The assigned IP address of the controlled computer in the LAN.
- **Status** - Indicates whether or not the MAC and IP addresses are bound.
- **Configure** - Load or delete an item.
  - Load - Load the item to the IP & MAC Binding list.
  - Delete - Delete the item.

Click the Bind All button to bind all the current items, available after enable.

Click the Load All button to load all items to the IP & MAC Binding list.

Click the Refresh button to refresh all items.

NOTE: An item could not be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before. Error warning will prompt as well. Likewise, "Load All" only loads the items without interference to the IP & MAC Binding list.

QUICK SETUP

Please refer to "Quick Installation Guide" on page 26.

5 NETWORK SETTINGS

There are five submenus under the Network menu: WAN, MAC Clone, LAN, Dynamic DNS and Binding Settings. Click any of them, and you will be able to configure the corresponding function.

WAN

Choose menu "Network->WAN", you can configure the IP parameters of the WAN on the screen below.

If your ISP provides the DHCP service, please choose Dynamic IP type, and the Router will automatically get IP parameters from your ISP. You can see the page as follows.

Figure 18: WAN-Dynamic IP

This page displays the WAN IP parameters assigned dynamically by your ISP, including IP address, Subnet Mask, Default Gateway, etc. Click the Renew button to renew the IP parameters from your ISP. Click the Release button to release the IP parameters.

- **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU Size unless required by your ISP.

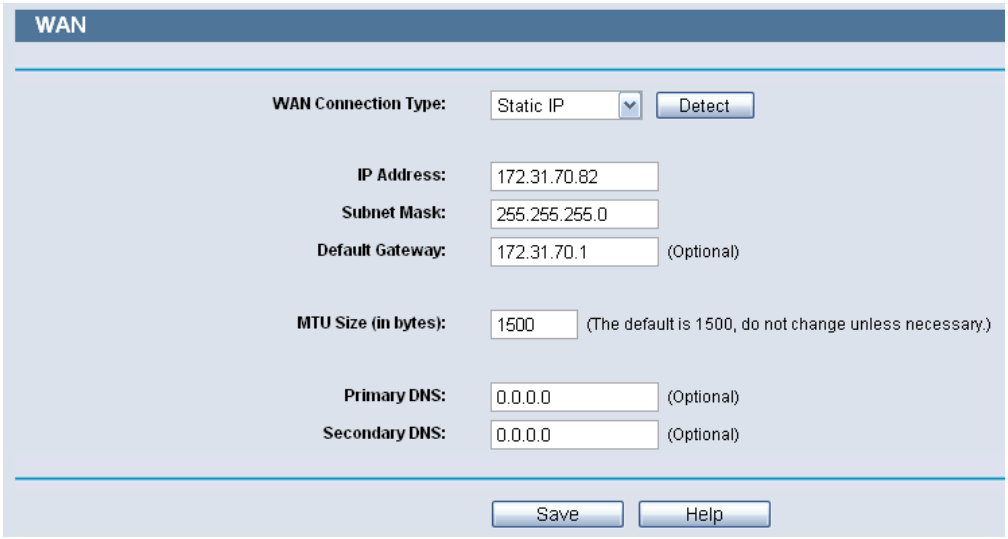
- **Use These DNS Servers** - If your ISP gives you one or two DNS addresses, select Use These DNS Servers and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from your ISP.

NOTE: If you find error when you go to a Web site after entering the DNS addresses, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

- **Get IP with Unicast DHCP** - A few ISPs' DHCP servers do not support the broadcast applications. If you cannot get the IP Address normally, you can choose this option. (It is rarely required.)

If your ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting, select Static IP. The Static IP settings page will appear.

Figure 19: WAN-Static IP



- **IP Address** - Enter the IP address in dotted-decimal notation provided by your ISP.

- **Subnet Mask** - Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.

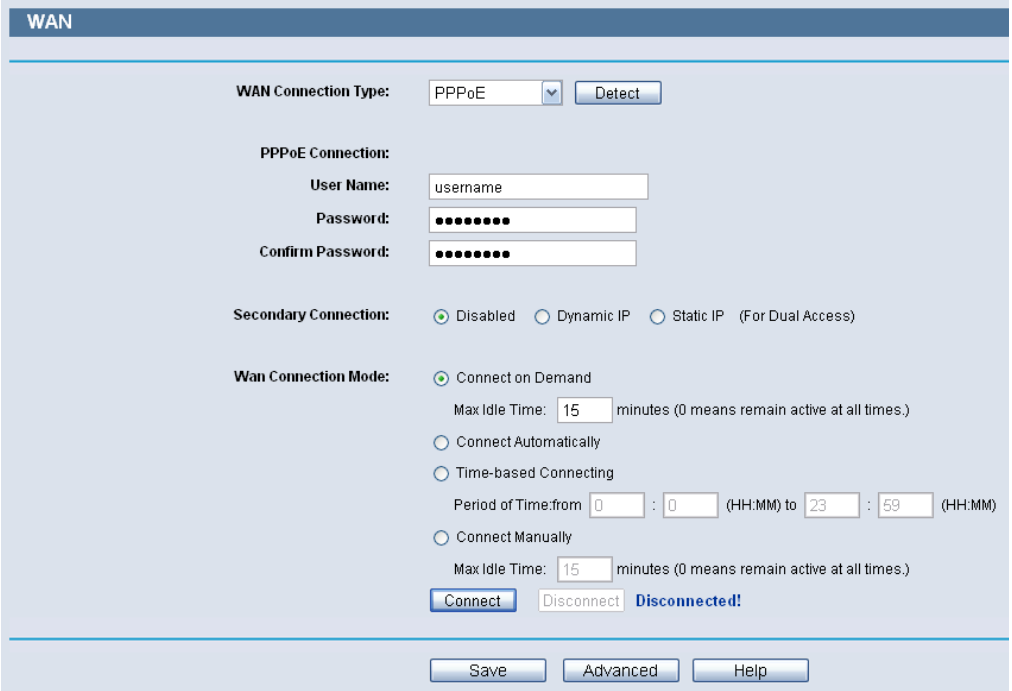
- **Default Gateway** - (Optional) Enter the gateway IP address in dotted-decimal notation provided by your ISP.

- **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU Size unless required by your ISP.

- **Primary/Secondary DNS** - (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.

If your ISP provides a PPPoE connection, select PPPoE option, then enter the following parameters:

Figure 20: WAN-PPPoE



- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

- **Secondary Connection** - It's available only for PPPoE Connection. If your ISP provides an extra Connection type such as Dynamic/Static IP to connect to a local area network, then you can check the radio button of Dynamic/Static IP to activate this secondary connection.

  - **Disabled** - The Secondary Connection is disabled by default, so there is PPPoE connection only. This is recommended.

  - **Dynamic IP** - You can check this radio button to use Dynamic IP as the secondary connection to connect to the local area network provided by ISP.

  - **Static IP** - You can check this radio button to use Static IP as the secondary connection to connect to the local area network provided by ISP.

- **Connect on Demand** - In this mode, the Internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the Internet again. If you want your Internet connection keeps active all the time, please enter "0" in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.

- **Connect Automatically** - The connection can be re-established automatically when it was down.

- **Time-based Connecting** - The connection will only be established in the period from the start time to the end time (both are in HH:MM format).

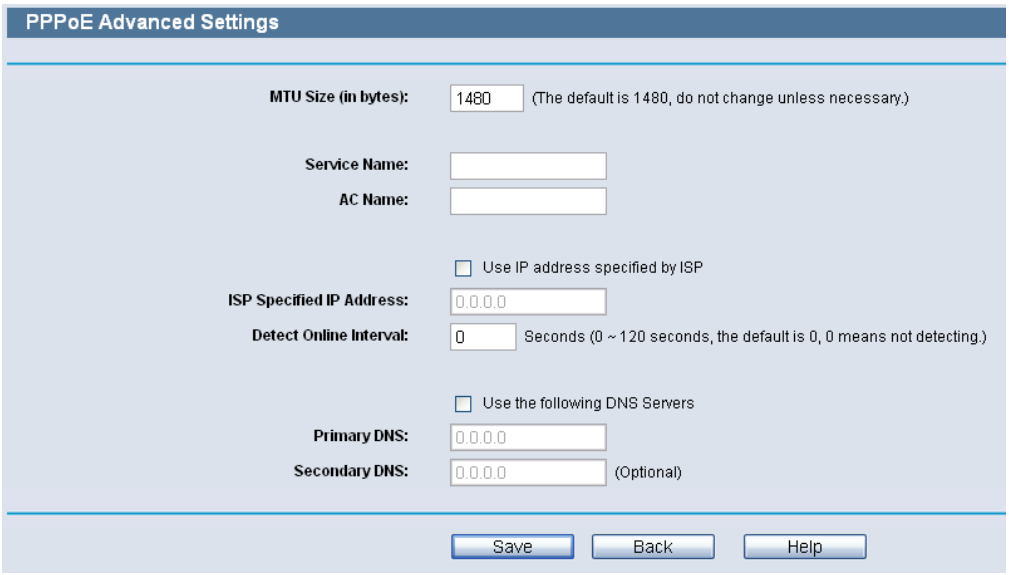
NOTE: Only when you have configured the system time on System Tools -> Time page, will the Time-based Connecting function can take effect.

- **Connect Manually** - You can click the Connect/ Disconnect button to connect/disconnect immediately. This mode also supports the Max Idle Time function as Connect on Demand mode. The Internet connection can be disconnected automatically after a specified inactivity period and re-established when you attempt to access the Internet again.

CAUTION: Sometimes the connection cannot be terminated even though you specify a Max Idle Time, since some applications are visiting the Internet continually in the background.

If you want to do some advanced configurations, please click the Advanced button, and the advanced settings page will appear:

Figure 21: WAN-PPPoE Advanced Settings

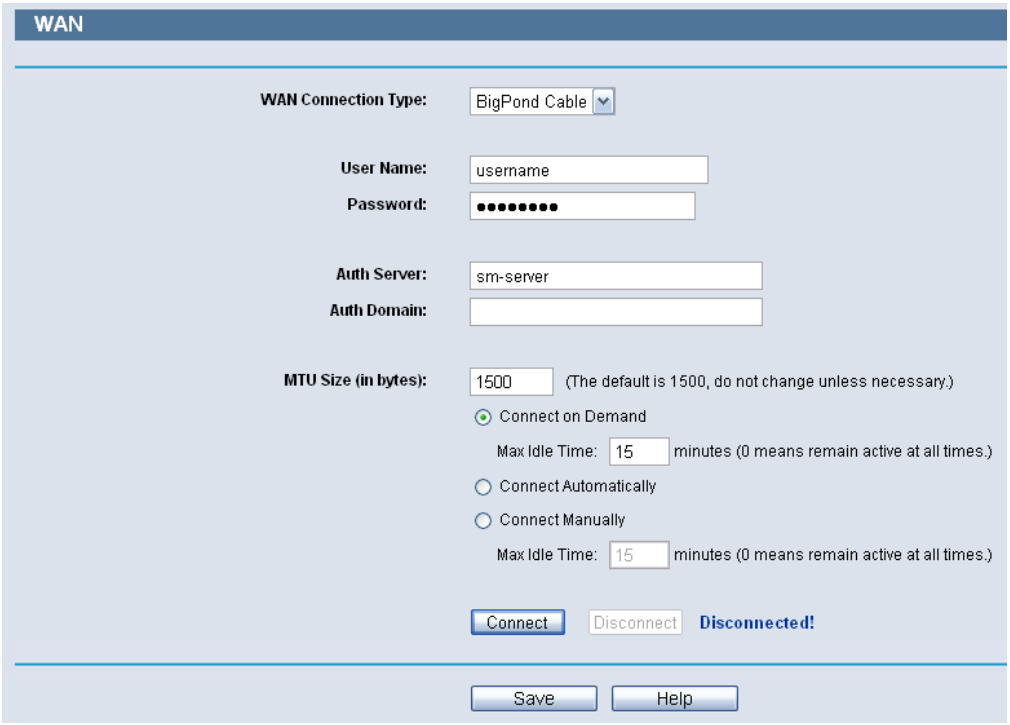


- **MTU Size** - The default MTU size is "1480" bytes, which is usually fine. It is not recommended that you change the default MTU Size unless required by your ISP.
- **Service Name/AC Name** - The service name and AC (Access Concentrator) name, which should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.
- **ISP Specified IP Address** - If your ISP does not automatically assign IP addresses to the Router during login, please click "Use IP address specified by ISP" check box and enter the IP address provided by your ISP in dotted-decimal notation.
- **Detect Online Interval** - The Router will detect Access Concentrator online at every interval. The default value is "0". You can input the value between "0"and "120". The value "0" means no detect.
- **DNS IP address** - If your ISP does not automatically assign DNS addresses to the Router during login, please click "Use the following DNS servers" check box and enter the IP address in dotted-decimal notation of your ISP's primary DNS server. If a secondary DNS server address is available, enter it as well.

Click the Save button to save your settings.

If your ISP provides BigPond Cable (or Heart Beat Signal) connection, please select BigPond Cable, then enter the following parameters:

Figure 22: WAN-BigPond Cable



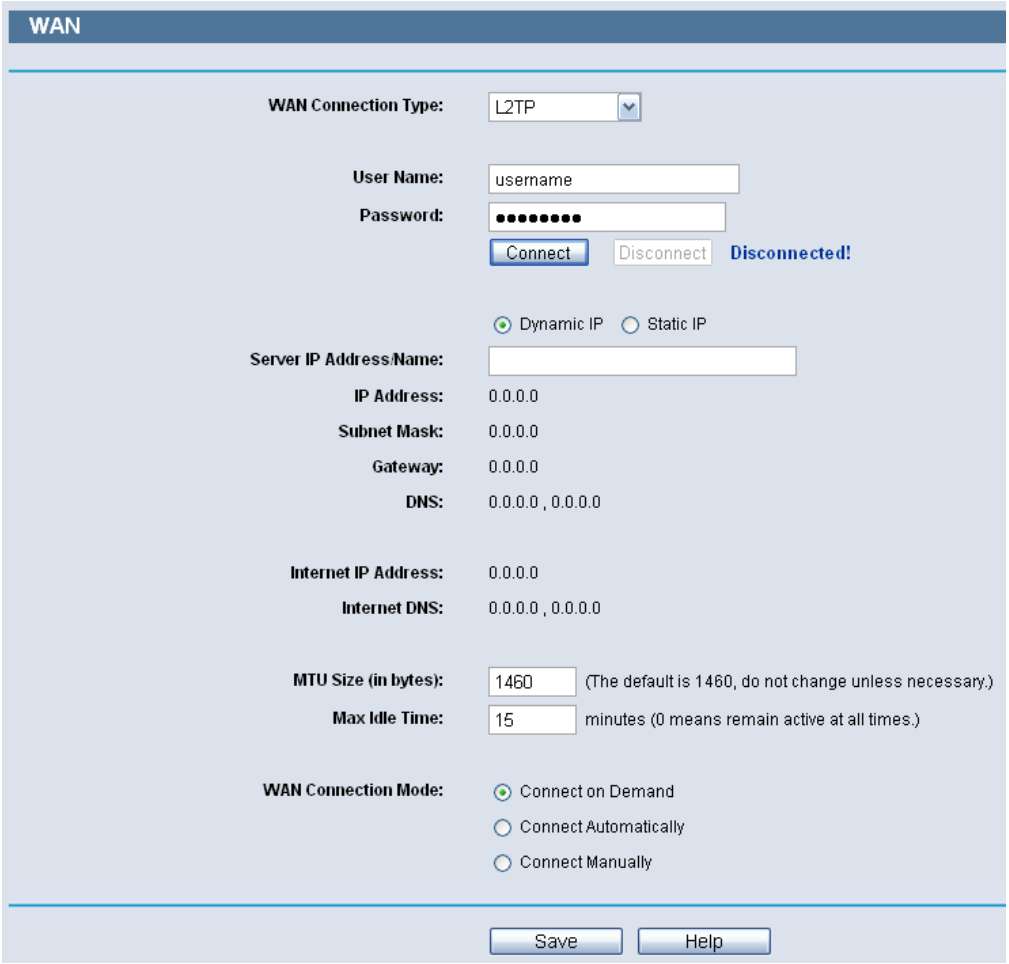
- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Auth Server** - Enter the authenticating server IP address or host name.
- **Auth Domain** - Type in the domain suffix server name based on your location.

  For example:
  NSW / ACT - nsw.bigpond.net.au
  VIC / TAS / WA / SA / NT - vic.bigpond.net.au
  QLD - qld.bigpond.net.au
- **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU Size unless required by your ISP.
- **Connect on Demand** - In this mode, the Internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be re-established when you attempt to access the Internet again. If you want your Internet connection keeps active all the time, please enter "0" in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.
- **Connect Automatically** - The connection can be re-established automatically when it was down.
- **Connect Manually** - You can click the Connect/Disconnect button to connect/disconnect immediately. This mode also supports the Max Idle Time function as Connect on Demand mode. The Internet connection can be disconnected automatically after a specified inactivity period and re-established when you attempt to access the Internet again. Click the Connect button to connect immediately. Click the Disconnect button to disconnect immediately.

CAUTION: Sometimes the connection cannot be terminated even though you specify a Max Idle Time because some applications may be visiting the Internet continually in the background.

If your ISP provides L2TP connection, please select L2TP option, then enter the following parameters :

Figure 23: WAN-L2TP



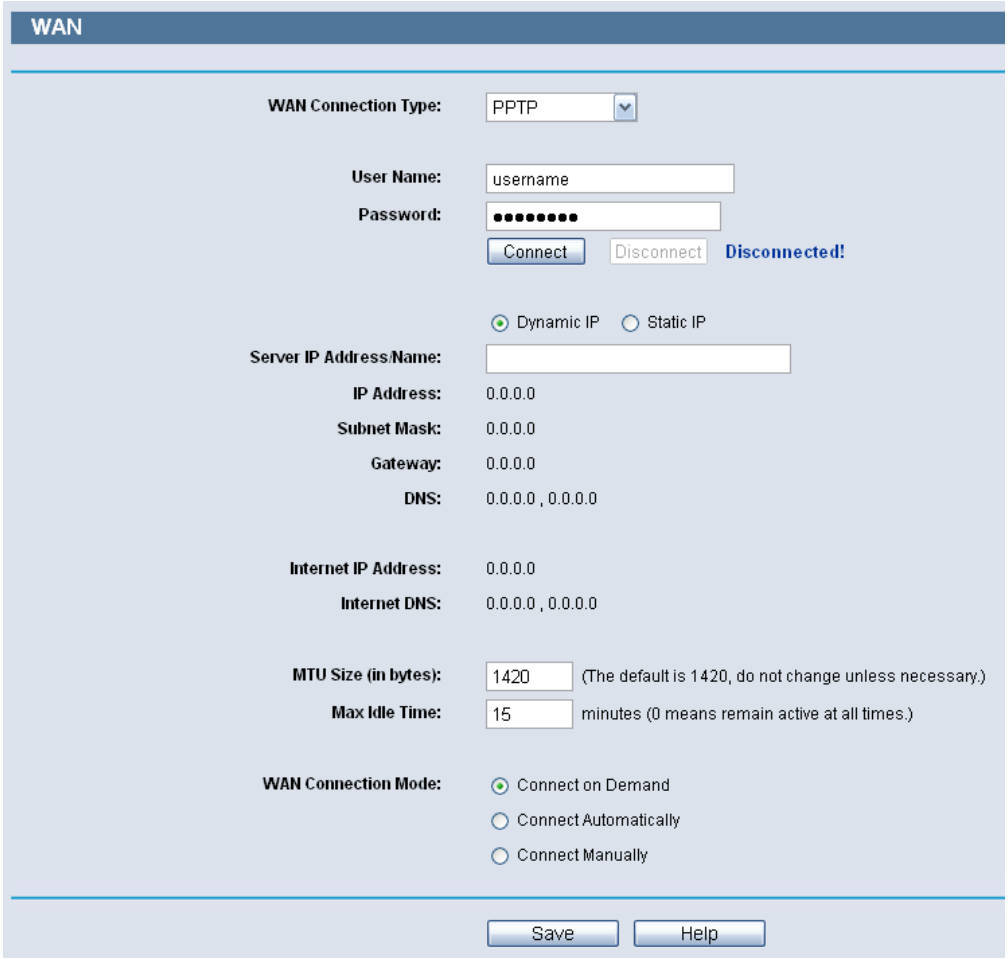
- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP** - Choose either as you are given by your ISP. Click the Connect button to connect immediately. Click the Disconnect button to disconnect immediately.
- **Connect on Demand** - You can configure the Router to disconnect from your Internet connection after a specified period of inactivity (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

- **Connect Automatically** - Connect automatically after the Router is disconnected. To use this option, click the radio button.
- **Connect Manually** - You can configure the Router to make it connect or disconnect manually. After a specified period of inactivity (Max Idle Time), the Router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the Max Idle Time field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

CAUTION: Sometimes the connection cannot be disconnected even though you specify a Max Idle Time, since some applications may be visiting the Internet continually in the background.

If your ISP provides PPTP connection, please select PPTP option, then enter the following parameters:

Figure 24: WAN-PPTP



- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

- **Dynamic IP/ Static IP** - Choose either as you are given by your ISP and enter the ISP's IP address or the domain name. If you choose static IP and enter the domain name, you should also enter the DNS assigned by your ISP. And click the Save button. Click the Connect button to connect immediately. Click the Disconnect button to disconnect immediately.

- **Connect on Demand** - You can configure the Router to disconnect from your Internet connection after a specified period of inactivity (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

- **Connect Automatically** - Connect automatically after the Router is disconnected. To use this option, click the radio button.

- **Connect Manually** - You can configure the Router to make it connect or disconnect manually. After a specified period of inactivity (Max Idle Time), the Router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the Max Idle Time field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

CAUTION: Sometimes the connection cannot be disconnected even though you specify a Max Idle Time, since some applications may be visiting the Internet continually in the background.

NOTE: If you do not know how to choose the appropriate connection type, click the Detect button to allow the Router to automatically search your Internet connection for servers and protocols. The connection type will be reported when an active Internet service is successfully detected by the Router. This report is for your reference only. To make sure the connection type your ISP provides, please refer to the ISP. The various types of Internet connections that the Router can detect are as follows:

  - PPPoE - Connections which use PPPoE that requires a user name and password.

  - Dynamic IP - Connections which use dynamic IP address assignment.

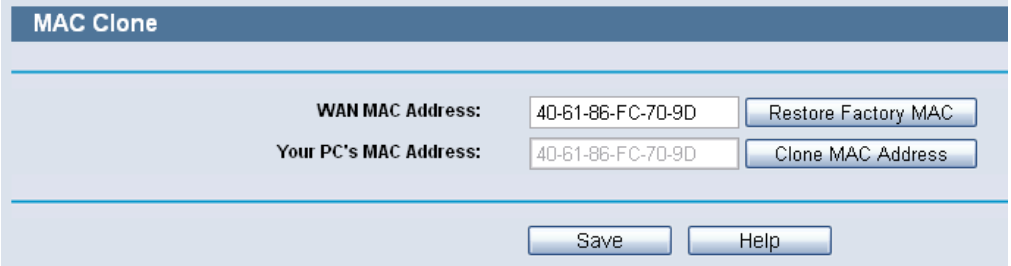
- Static IP - Connections which use static IP address assignment.

The Router can not detect PPTP/L2TP/BigPond connections with your ISP. If your ISP uses one of these protocols, then you must configure your connection manually.

MAC CLONE

Choose menu "Network->MAC Clone", you can configure the MAC address of the WAN on the screen below:

Figure 25: MAC Address Clone



Some ISPs require that you register the MAC Address of your adapter. Changes are rarely needed here.

- **WAN MAC Address** - This field displays the current MAC address of the WAN port. If your ISP requires you to register the MAC address, please enter the correct MAC address into this field in XX-XX-XX-XX-XX-XX format(X is any hexadecimal digit).
- **Your PC's MAC Address** - This field displays the MAC address of the PC that is managing the Router. If the MAC address is required, you can click the Clone MAC Address To button and this MAC address will fill in the WAN MAC Address field.

Click Restore Factory MAC to restore the MAC address of WAN port to the factory default value.

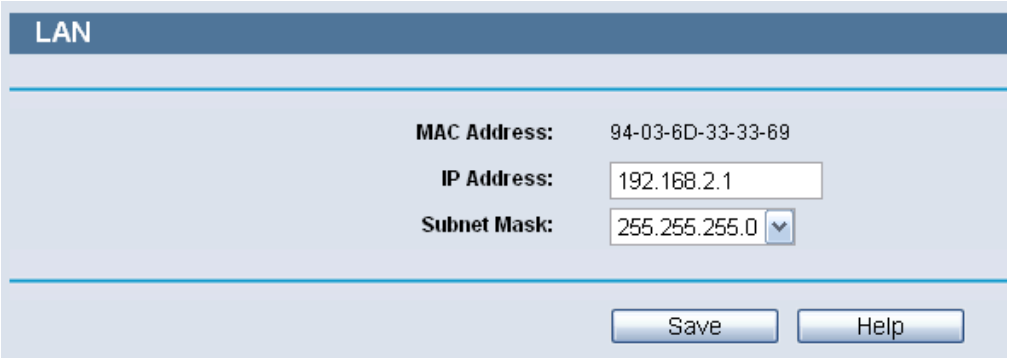
Click the Save button to save your settings.

NOTE: Only the PC on your LAN can use the MAC Address Clone function.

LAN

Choose menu "Network->LAN", you can configure the IP parameters of the LAN on the screen as below.

Figure 26: LAN Settings



- **MAC Address** - The physical address of the Router, as seen from the LAN. The value can't be changed.
- **IP Address** - Enter the IP address of your Router or reset it in dotted-decimal notation (factory default: 192.168.2.1).
- **Subnet Mask** - An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

NOTE: If you change the IP Address of LAN, you must use the new IP Address to login the Router.

NOTE: If the new LAN IP Address you set is not in the same subnet, the IP Address pool of the DHCP server will change accordingly at the same time, while the Virtual Server and DMZ Host will not take effect until they are re-configured.

DYNAMIC DNS

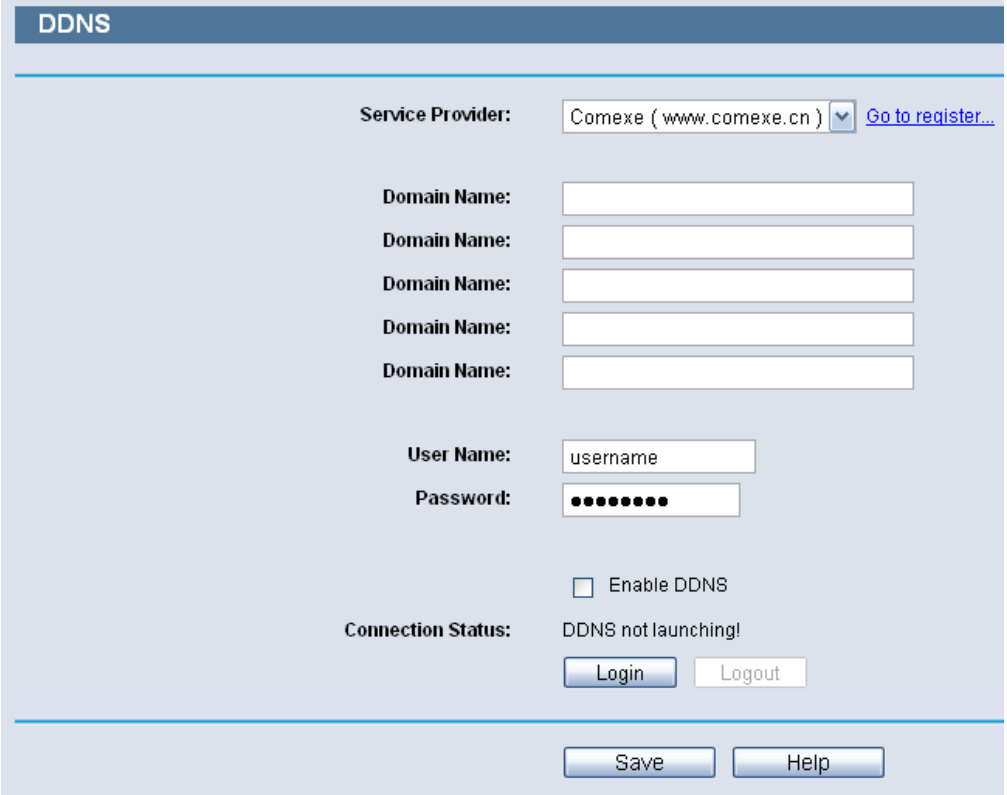
Choose menu "Dynamic DNS", and configure the Dynamic DNS function.

The Router offers the DDNS (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as www.comexe.cn, www.dyndns.org, or www.no-ip.com. The Dynamic DNS client service provider will give you a password or key.

COMEXE.CN DDNS

If the dynamic DNS Service Provider you select is www.comexe.cn, the page will appear.

Figure 27: Comexe.cn DDNS Settings



To set up for DDNS, follow these instructions:

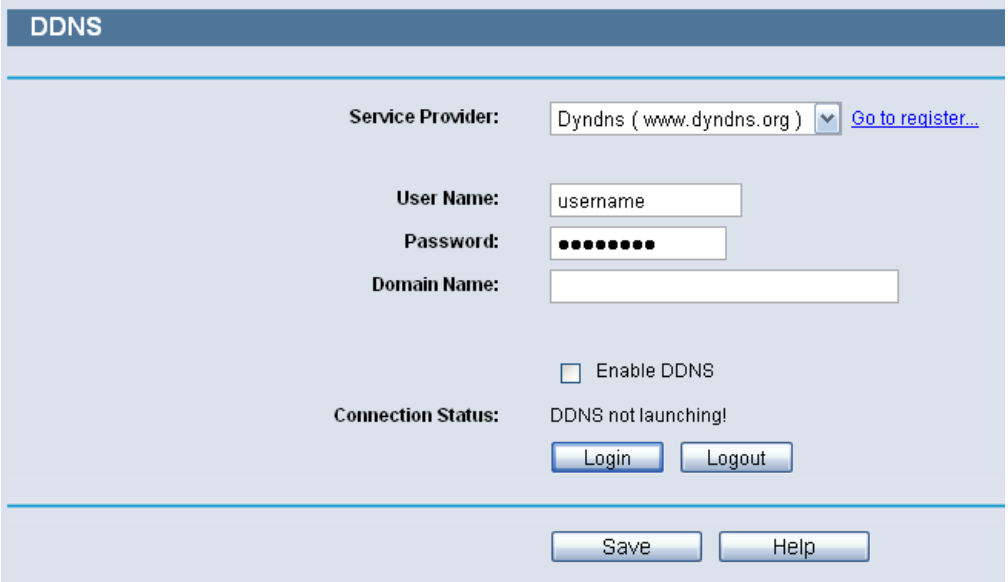
1. Type the Domain Name received from your dynamic DNS service provider.
2. Type the User Name for your DDNS account.
3. Type the Password for your DDNS account.
4. Click the Login button to log in to the DDNS service.
   - Connection Status -The status of the DDNS service connection is displayed here.

Click Logout to log out of the DDNS service.

DYNDNS.ORG DDNS

If the dynamic DNS Service Provider you select is www.dyndns.org, the page will appear.

Figure 28: Dyndns.org DDNS Settings



To set up for DDNS, follow these instructions:

1. Type the User Name for your DDNS account.
2. Type the Password for your DDNS account.
3. Type the Domain Name you received from dynamic DNS service provider here.
4. Click the Login button to log in to the DDNS service.

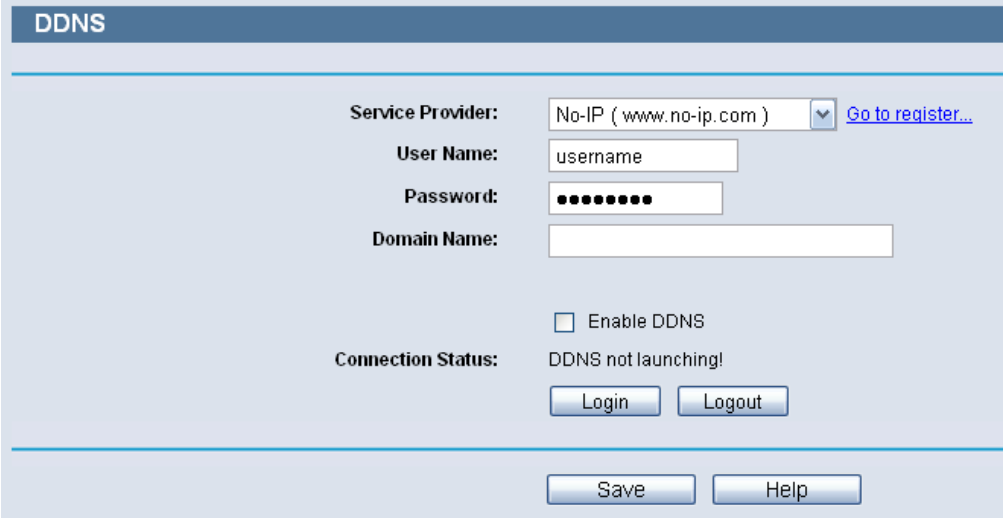
- Connection Status - The status of the DDNS service connection is displayed here.

Click Logout to logout of the DDNS service.

NO-IP.COM DDNS

If the dynamic DNS Service Provider you select is www.no-ip.com, the page will appear.

Figure 29: No-ip.com DDNS Settings



To set up for DDNS, follow these instructions:

1. Type the User Name for your DDNS account.
2. Type the Password for your DDNS account.
3. Type the Domain Name you received from dynamic DNS service provider.
4. Click the Login button to log in the DDNS service.

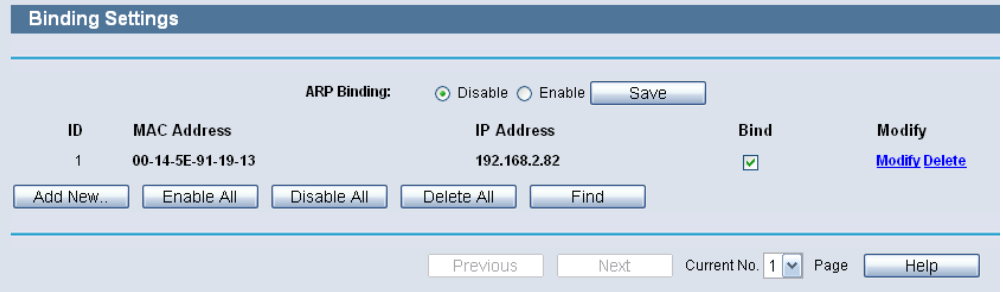
- Connection Status - The status of the DDNS service connection is displayed here.

Click Logout to log out the DDNS service.

BINDING SETTING

This page displays the IP & MAC Binding Setting table; you can operate it in accord with your desire.

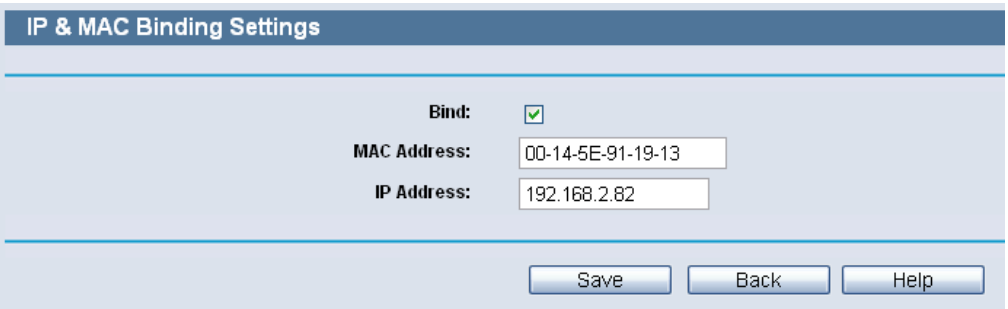
Figure 30: Binding Settings



- **MAC Address** - The MAC address of the controlled computer in the LAN.
- **IP Address** - The assigned IP address of the controlled computer in the LAN.
- **Bind** - Check this option to enable ARP binding for a specific device.
- **Modify** - To modify or delete an existing entry.

When you want to add or modify an IP & MAC Binding entry, you can click the Add New button or Modify button, and then you will go to the next page. This page is used for adding or modifying an IP & MAC Binding entry .

Figure 31: IP & MAC Binding Settings (Add & Modify)



To add IP & MAC Binding entries, follow the steps below.

1. Click the Add New.
2. Enter the MAC Address and IP Address.
3. Select the Bind checkbox.

4. Click the Save button to save it.

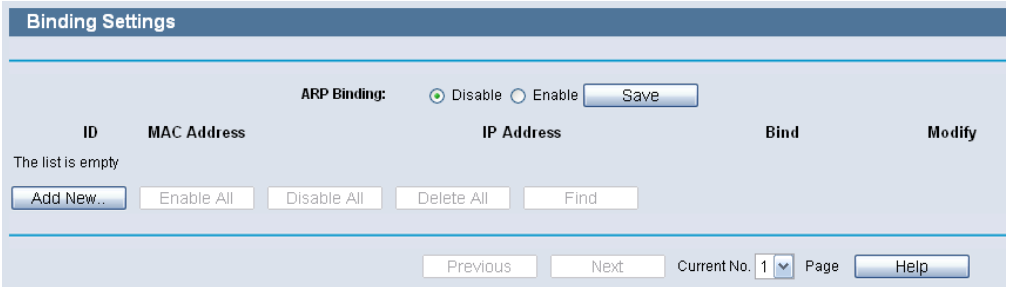
To modify or delete an existing entry, follow the steps below.

1. Find the desired entry in the table.
2. Click Modify or Delete as desired on the Modify column.

To find an existing entry, follow the steps below.

1. Click the Find button.
2. Enter the MAC Address or IP Address.
3. Click the Find button in the page as shown in the following figure.

Figure 32: Find IP & MAC Binding Entry



Click the Enable All button to make all entries enabled.

Click the Delete All button to delete all entries.

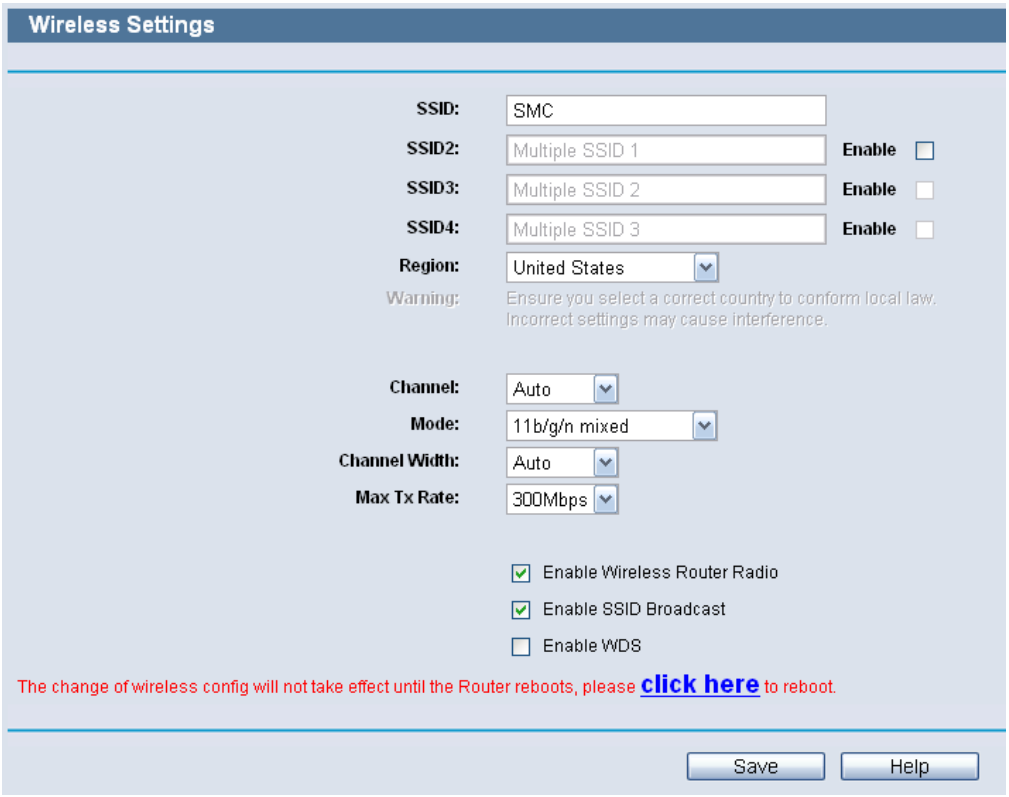
6 WIRELESS SETTINGS

There are six submenus under the Wireless menu: Wireless Settings, Wireless Security, Wireless MAC Filtering, Wireless Advanced, Wireless Statistics and WPS. Click any of them, and you will be able to configure the corresponding function.

WIRELESS SETTINGS

Choose menu "Wireless->Wireless Setting", you can configure the basic settings for the wireless network on this page.

Figure 33: Wireless Settings



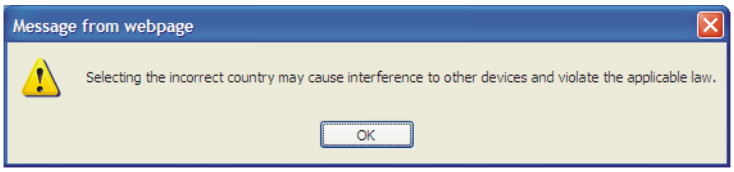
- **SSID** - Enter a value of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security, the default SSID is set to be "SMC". This value is case-sensitive. For example, "TEST" is NOT the same as "test".

- **SSID (2-4)** - Up to 4 SSIDs for each BSS can be set, the name can be up to 32 characters. The Multi-SSID function is available only when Enable is checked.

- **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the Router can be used. It may be illegal to use the wireless function of the Router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

When you select your local region from the pull-down list, click the Save button, then the Note Dialog appears. Click OK.

Figure 34: Note Dialog


Message from webpage
Selecting the incorrect country may cause interference to other devices and violate the applicable law.
OK

NOTE: Limited by local law regulations, version for North America does not have region selection option.

- **Channel** - This field determines which operating frequency will be used. The default channel is set to Auto, so the AP will choose the best channel automatically. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

- **Mode** - Select the desired mode. The default setting is 11bgn mixed.

  - 11b only - Select if all of your wireless clients are 802.11b.
  - 11g only - Select if all of your wireless clients are 802.11g.
  - 11n only- Select only if all of your wireless clients are 802.11n.
  - 11b/g mixed - Select if you are using both 802.11b and 802.11g wireless clients.
  - 11b/g/n mixed - Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.

Select the desired wireless mode. When 802.11g mode is selected, only 802.11g wireless stations can connect to the Router. When 802.11n mode is selected, only 802.11n wireless stations can connect to the AP. It is strongly recommended that you set the Mode to 11b/g/n mixed, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the Router.

- **Channel width** - Select any channel width from the pull-down list. The default setting is automatic, which can adjust the channel width for your clients automatically.

NOTE: If 11b only, 11g only, or 11bg mixed is selected in the Mode field, the Channel Width selecting field will turn grey and the value will become 20M, which is unable to be changed.

- **Max Tx Rate** - You can limit the maximum tx rate of the Router through this field.
- **Enable Wireless Router Radio** - The wireless radio of this Router can be enabled or disabled to allow wireless stations access.
- **Enable SSID Broadcast** - When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. If you select the Enable SSID Broadcast checkbox, the Wireless Router will broadcast its name (SSID) on the air.

WIRELESS SECURITY

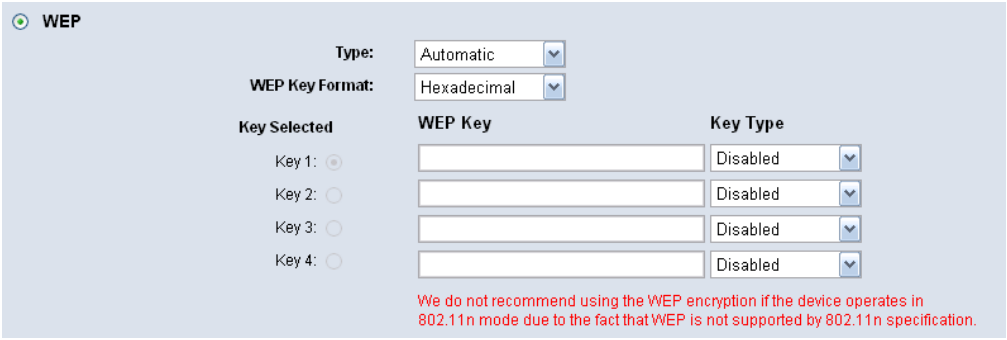
Choose menu "Wireless->Wireless Security", you can configure the security settings of your wireless network.

There are five wireless security modes supported by the Router: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2), WPA2-PSK (Pre-Shared Key), WPA-PSK (Pre-Shared Key).

Figure 35: Wireless Security

- **Disable Security** - If you do not want to use wireless security, select this check box, but it's strongly recommended to choose one of the following modes to enable security.
- **WEP** - It is based on the IEEE 802.11 standard. If you select this check box, you will find a notice in red as show in the following figure.

Figure 36: WEP



- Type - you can choose the type for the WEP security on the pull-down list. The default setting is Automatic, which can select Open System or Shared Key authentication type automatically based on the wireless station's capability and request.

- WEP Key Format - Hexadecimal and ASCII formats are provided. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. ASCII format stands for any combination of keyboard characters in the specified length.

- WEP Key- Select which of the four keys will be used and enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your network.

- Key Type - You can select the WEP key length (64-bit, or 128-bit, or 152-bit.) for encryption. "Disabled" means this WEP key entry is invalid.

  64-bit - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 5 ASCII characters.

  128-bit - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 13 ASCII characters.

  152-bit - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 16 ASCII characters.

NOTE: If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

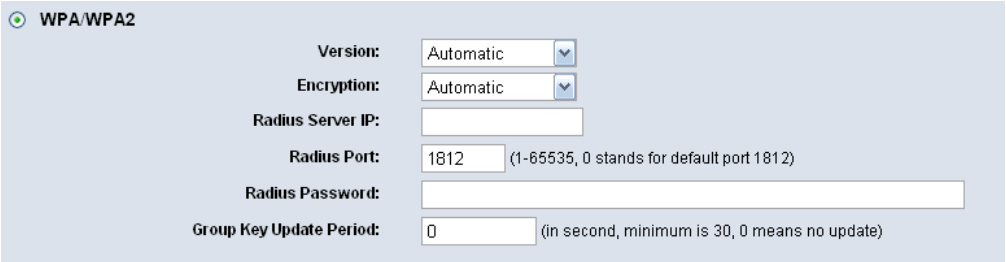
- **WPA /WPA2** - It's based on Radius Server.

  - Version - you can choose the version of the WPA security on the pull-down list. The default setting is Automatic, which can select WPA (Wi-Fi Protected Access) or WPA2 (WPA version 2) automatically based on the wireless station's capability and request.

  - Encryption - You can select either Automatic, or TKIP or AES.

NOTE: If you check the WPA/WPA2 radio button and choose TKIP encryption, you will find a notice in red.

Figure 37: WPA/WPA2



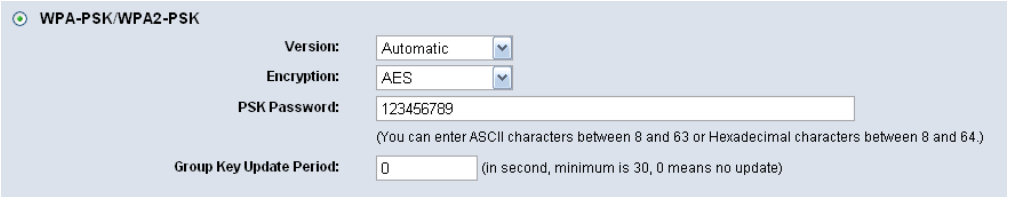
- Radius Server IP - Enter the IP address of the Radius Server.
- Radius Port - Enter the port that radius service used.
- Radius Password - Enter the password for the Radius Server.
- Group Key Update Period - Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

◆ **WPA-PSK/WPA2-PSK** - It's the WPA/WPA2 authentication type based on pre-shared passphrase.

- Version - you can choose the version of the WPA-PSK security on the drop-down list. The default setting is Automatic, which can select WPA-PSK (Pre-shared key of WPA) or WPA2-PSK (Pre-shared key of WPA) automatically based on the wireless station's capability and request.
- Encryption - When WPA-PSK or WPA is set as the Authentication Type, you can select either Automatic, or TKIP or AES as Encryption.

NOTE: If you check the WPA-PSK/WPA2-PSK radio button and choose TKIP encryption, you will find a notice in red.

Figure 38: WPA-PSK/WPA2-PSK



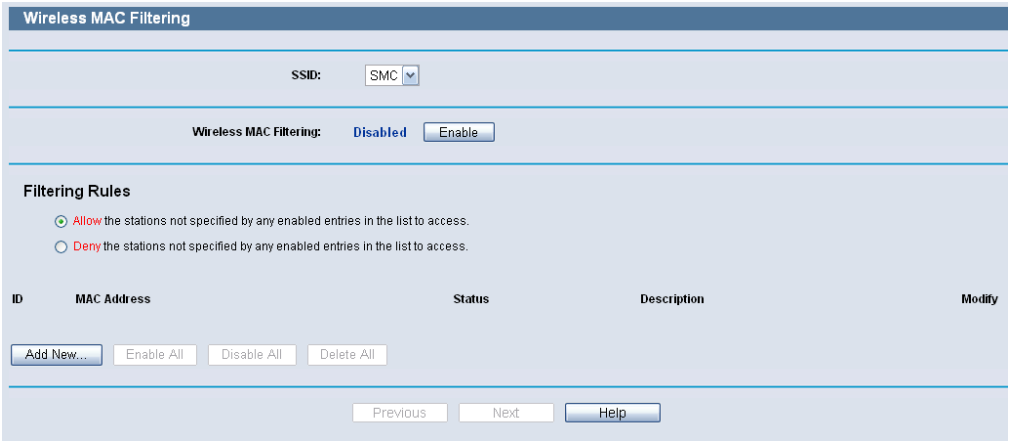
- PSK Passphrase - You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters.
- Group Key Update Period - Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

Be sure to click the Save button to save your settings on this page.

WIRELESS MAC FILTERING

Choose menu "Wireless->MAC Filtering", you can control the wireless access by configuring the Wireless MAC Address Filtering function.

Figure 39: Wireless MAC Address Filtering

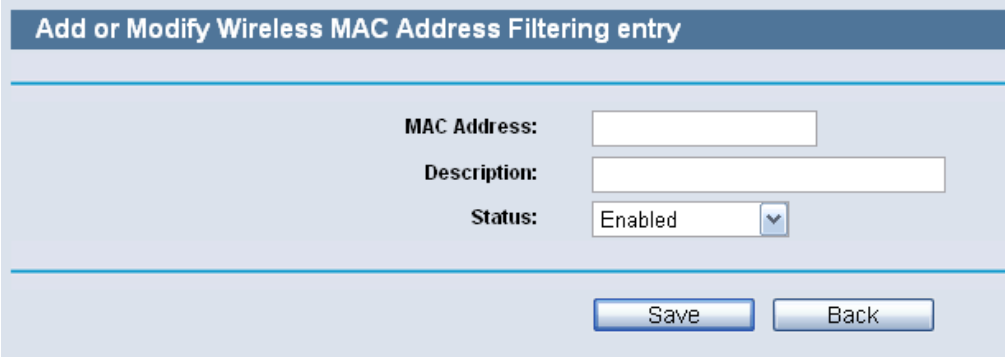


To filter wireless users by MAC Address, click Enable. The default setting is Disable.

- **MAC Address** - The wireless station's MAC address that you want to filter.
- **Status** - The status of this entry either Enabled or Disabled.
- **Description** - A simple description of the wireless station.

To Add a Wireless MAC Address filtering entry, click the Add New button. The "Add or Modify Wireless MAC Address Filtering entry" page will appear:

Figure 40: Add or Modify Wireless MAC Address Filtering Entry



To add or modify a MAC Address Filtering entry, follow these instructions:

1. Enter the appropriate MAC Address into the MAC Address field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0A-EB-00-07-8A.

2. Enter a simple description of the wireless station in the Description field. For example: Wireless station A.

3. Status - Select Enabled or Disabled for this entry on the Status pull-down list.

4. Click the Save button to save this entry.

To modify or delete an existing entry:

1. Click the Modify in the entry you want to modify. If you want to delete the entry, click the Delete.

2. Modify the information.

3. Click the Save button.

Click the Enable All button to make all entries enabled

Click the Disabled All button to make all entries disabled.

Click the Delete All button to delete all entries

Click the Next button to go to the next page

Click the Previous button to return to the previous page.

For example: If you desire that the wireless station A with MAC address 00-0A-EB-00-07-8A and the wireless station B with MAC address 00-0A-EB-00-23-11 are able to access the Router, but all the other wireless stations cannot access the Router, you can configure the Wireless MAC Address Filtering list by following these steps:

1. Click the Enable button to enable this function.

2. Select the radio button: Deny the stations not specified by any enabled entries in the list to access for Filtering Rules.

3. Delete all or disable all entries if there are any entries already.

4. Click the Add New button and enter the MAC address 00-0A-EB-00-07-8A /00-0A-EB-00-23-11 in the MAC Address field, then enter wireless station A/B in the Description field, while select Enabled in the Status pull-down list. Finally, click the Save and the Back button.

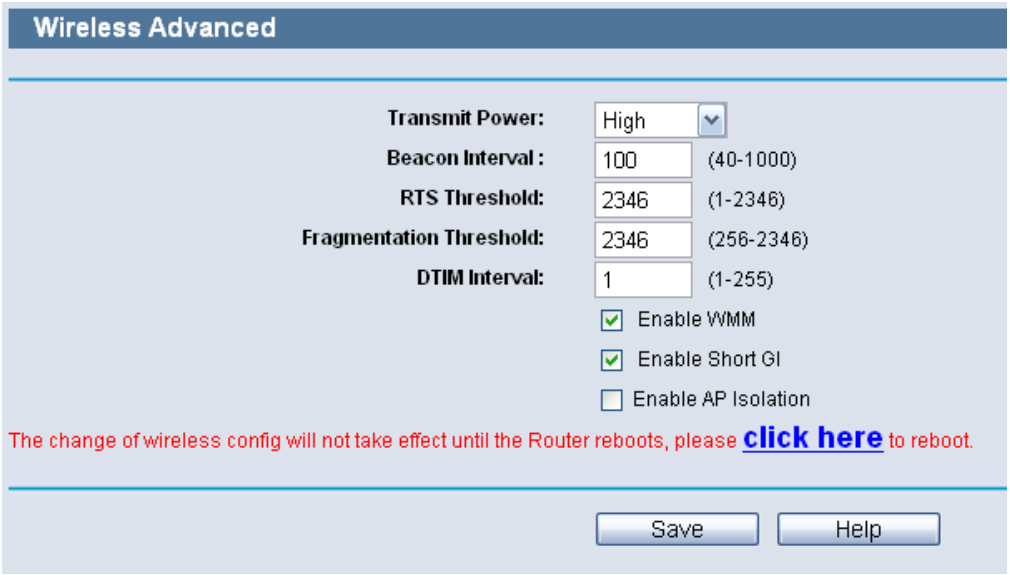
The filtering rules that configured should be similar to the following list:

Figure 41: Filtering Rules

WIRELESS ADVANCED

Choose menu "Wireless->Wireless Advanced", you can configure the advanced settings of your wireless network.

Figure 42: Wireless Advanced



- **Transmit Power** - Here you can specify the transmit power of Router. You can select High, Middle or Low which you would like. High is the default setting and is recommended.

- **Beacon Interval** - Enter a value between 20-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the router

to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.

- **RTS Threshold** - Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.

- **Fragmentation Threshold** - This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets. 2346 is the default setting and is recommended.

- **DTIM Interval** - This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.

- **Enable WMM** - WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended enabled.

- **Enable Short GI** - This function is recommended for it will increase the data capacity by reducing the guard interval time.

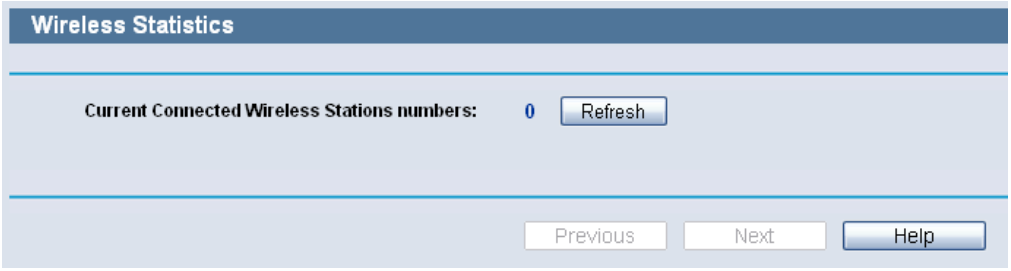
- **Enabled AP Isolation** - This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the Router but not with each other. To use this function, check this box. AP Isolation is disabled by default.

NOTE: If you are not familiar with the setting items in this page, it's strongly recommended to keep the provided default values; otherwise it may result in lower wireless network performance.

WIRELESS STATISTICS

Choose menu "Wireless->Wireless Statistics", you can see the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.

Figure 43: Wireless Statistics



- **MAC Address** - The connected wireless station's MAC address.
- **Current Status** - The connected wireless station's running status, one of STA-AUTH / STA-ASSOC / STA-JOINED / WPA / WPA-PSK / WPA2 / WPA2-PSK / AP-UP / AP-DOWN / Disconnected.
- **Received Packets** - Packets received by the station.
- **Sent Packets** - Packets sent by the station.

You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the Refresh button.

If the numbers of connected wireless stations go beyond one page, click the Next button to go to the next page and click the Previous button to return the previous page.

NOTE: This page will be refreshed automatically every 5 seconds.

WPS

This section will guide you add a new wireless device to an existing network quickly by WPS (Wi-Fi Protected Setup) function.

1. Choose menu "WPS", you will see the next screen.

Figure 44: WPS

- **WPS Status** - Enable or disable the WPS function here.
- **Current PIN** - The current value of the Router's PIN displayed here. The default PIN of the Router can be found in the label or User Guide.
- **Restore PIN** - Restore the PIN of the Router to its default.
- **Gen New PIN** - Click this button, and then you can get a new random value for the Router's PIN. You can ensure the network security by generating a new PIN.
- **Add device** - You can add the new device to the existing network manually by clicking this button.

2. Add a new device:

If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless adapter and Router using either Push Button Configuration (PBC) method or PIN method.

NOTE: To build a successful connection by WPS, you should also do the corresponding configuration of the new device for WPS function meanwhile.

For the configuration of the new device, here takes the Wireless Adapter of our company for example.

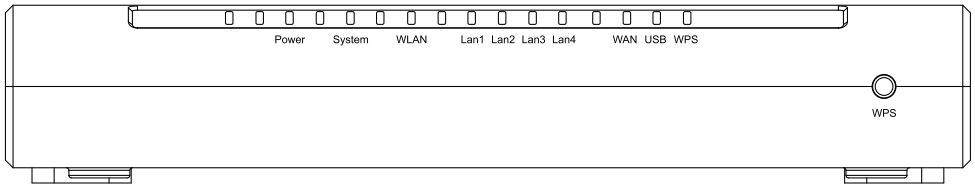
By PBC:

If the wireless adapter supports Wi-Fi Protected Setup and the Push Button Configuration (PBC) method, you can add it to the network by PBC with the following two methods.

Method One:

1. Press the WPS button on the front panel of the Router.

Figure 45: WPS button



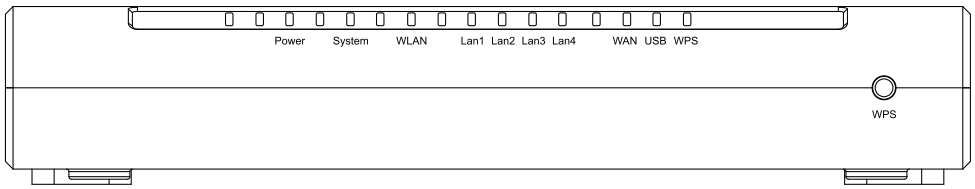
2. Press and hold the WPS button of the adapter directly for 2 or 3 seconds, then the adapter will connect to the router by WPS automatically.

Figure 46: WPS button

Method Two:

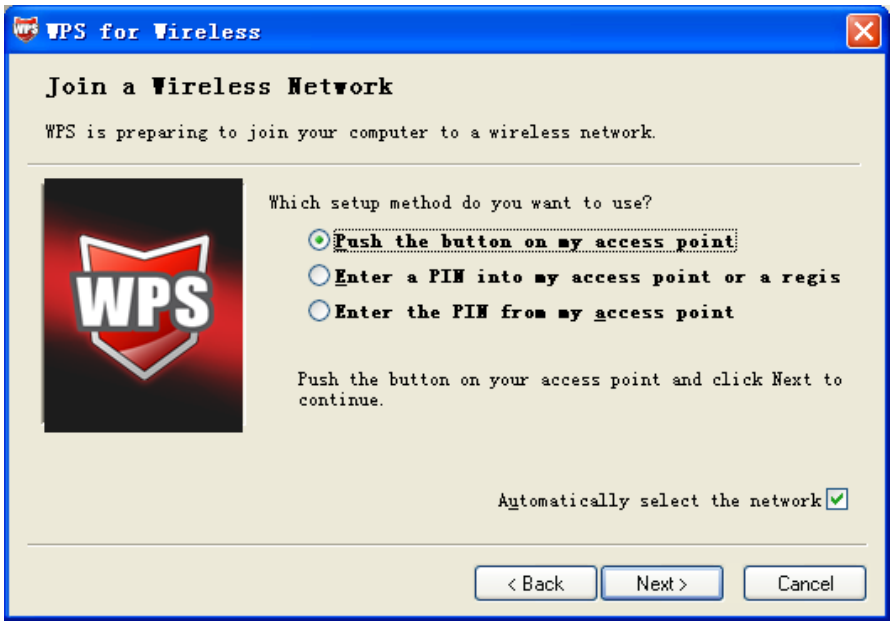
1. Press the WPS button on the front panel of the Router.

Figure 47: WPS button



2. For the configuration of the wireless adapter, please choose Push the button on my access point in the configuration utility of the WPS as below, and click Next.

Figure 48: The WPS Configuration Screen of Wireless Adapter


WPS for Wireless
Join a Wireless Network
WPS is preparing to join your computer to a wireless network.
Which setup method do you want to use?
Push the button on my access point
Enter a PIN into my access point or a regis
Enter the PIN from my access point
Push the button on your access point and click Next to continue.
Automatically select the network
< Back
Next >
Cancel

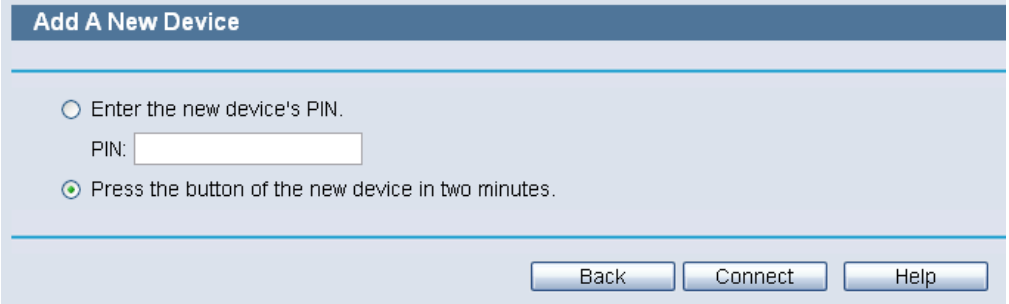
3. Wait for a while until the next screen appears. Click Finish to complete the WPS configuration.

Figure 49: The WPS Configuration Screen of Wireless Adapter

Method Three:

1. Keep the default WPS Status as Enabled and click the Add device button in Figure 44, then the following screen will appear.

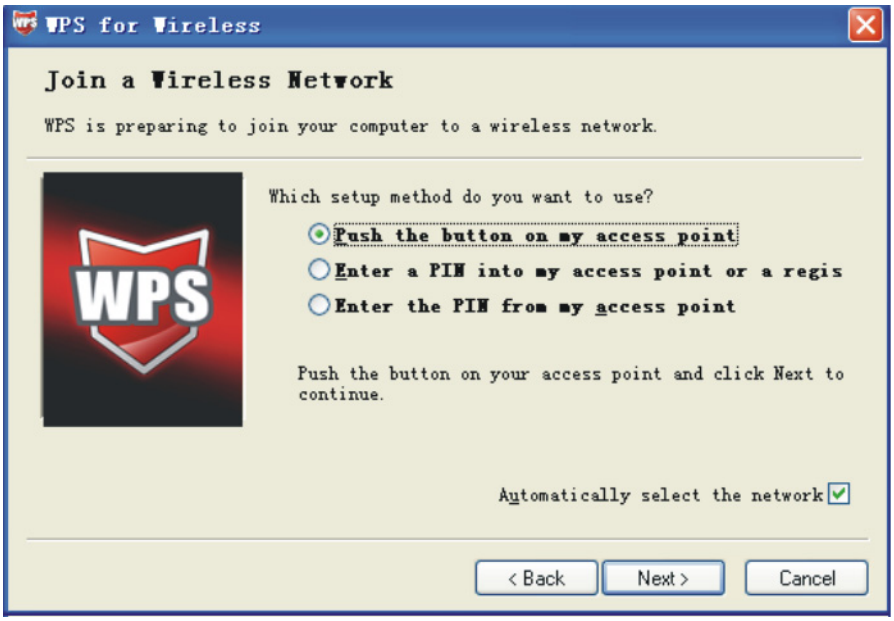
Figure 50: Add a New Device



2. Choose Press the button of the new device in two minutes and click Connect.

3. For the configuration of the wireless adapter, please choose Push the button on my access point in the configuration utility of the WPS as below, and click Next.

Figure 51: The WPS Configuration Screen of Wireless Adapter


WPS for Wireless
Join a Wireless Network
WPS is preparing to join your computer to a wireless network.
WPS
Which setup method do you want to use?
Push the button on my access point
Enter a PIN into my access point or a regis
Enter the PIN from my access point
Push the button on your access point and click Next to continue.
Automatically select the network
< Back
Next >
Cancel

4. Wait for a while until the next screen appears. Click Finish to complete the WPS configuration.

Figure 52: The WPS Configuration Screen of Wireless Adapter

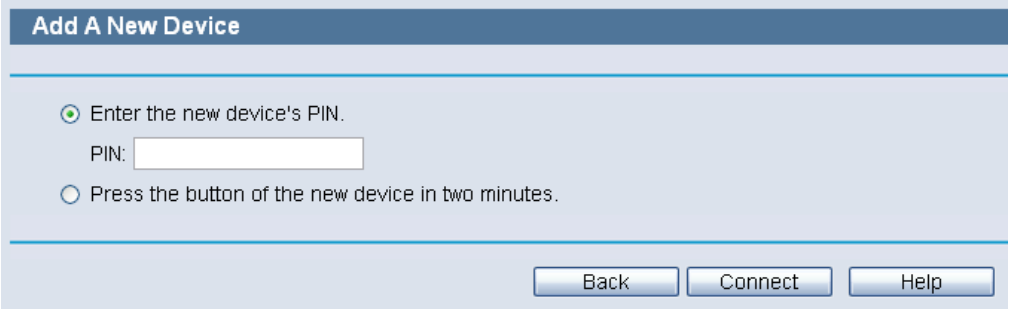
By PIN

If the new device supports Wi-Fi Protected Setup and the PIN method, you can add it to the network by PIN with the following two methods.

Method One: Enter the PIN into my Router

1. Keep the default WPS Status as Enabled and click the Add device button in Figure 44, then the following screen will appear.

Figure 53: Add a New Device

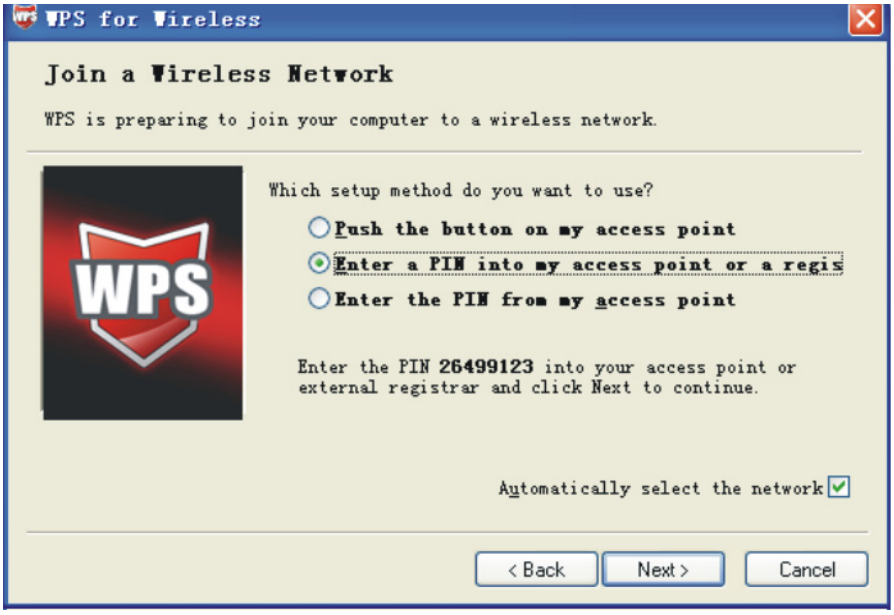


2. Choose Enter the new device's PIN and enter the PIN code of the wireless adapter in the field behind PIN in the above figure. Then click Connect.

NOTE: The PIN code of the adapter is always displayed on the WPS configuration screen.

3. For the configuration of the wireless adapter, please choose Enter a PIN into my access point or a registrar in the configuration utility of the WPS as below, and click Next.

Figure 54: The WPS Configuration Screen of Wireless Adapter


WPS for Wireless
Join a Wireless Network
WPS is preparing to join your computer to a wireless network.
WPS
Which setup method do you want to use?
Push the button on my access point
Enter a PIN into my access point or a regis
Enter the PIN from my access point
Enter the PIN 26499123 into your access point or external registrar and click Next to continue.
Automatically select the network
< Back
Next >
Cancel

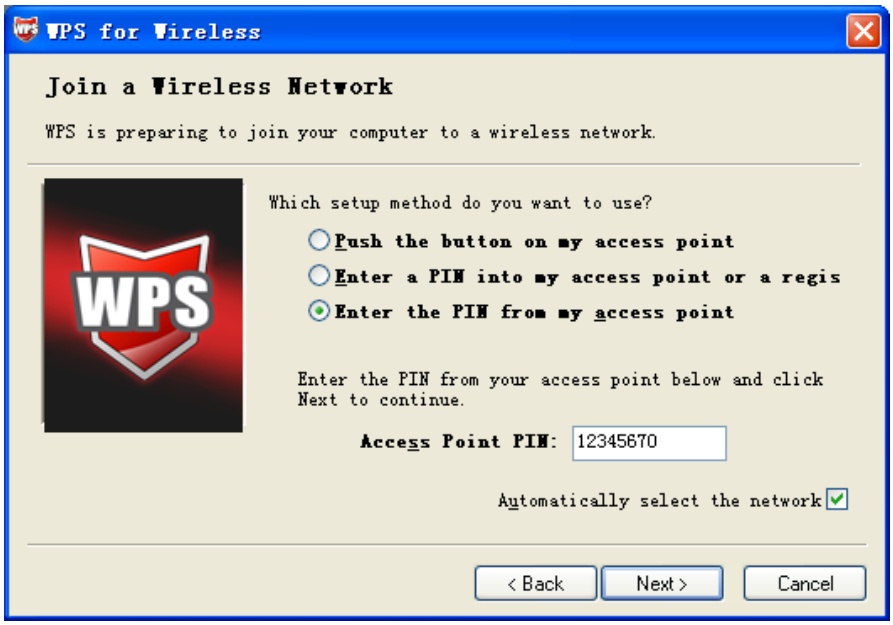
NOTE: In this example, the default PIN code of this adapter is 26499123 as the above figure shown.

Method Two: Enter the PIN from my Router

1. Get the Current PIN code of the Router. (Each router has its unique PIN code. Here takes the PIN code 12345670 of this Router for example).

2. For the configuration of the wireless adapter, please choose Enter a PIN from my access point in the configuration utility of the WPS as below, and enter the PIN code of the Router into the field behind Access Point PIN. Then click Next.

Figure 55: The WPS Configuration Screen of Wireless Adapter


WPS for Wireless
Join a Wireless Network
WPS is preparing to join your computer to a wireless network.
Which setup method do you want to use?
Push the button on my access point
Enter a PIN into my access point or a regis
Enter the PIN from my access point
Enter the PIN from your access point below and click Next to continue.
Access Point PIN: 12345670
Automatically select the network
< Back
Next >
Cancel

NOTE: The default PIN code of the Router can be found in its label or the WPS configuration screen as Figure 44.

3. Then the new device successfully connected to the network.

NOTE: The status LED on the Router will light green all the time if the device has been successfully added to the network.

The WPS function cannot be configured if the Wireless Function of the Router is disabled. Please make sure the Wireless Function is enabled before configuring the WPS.

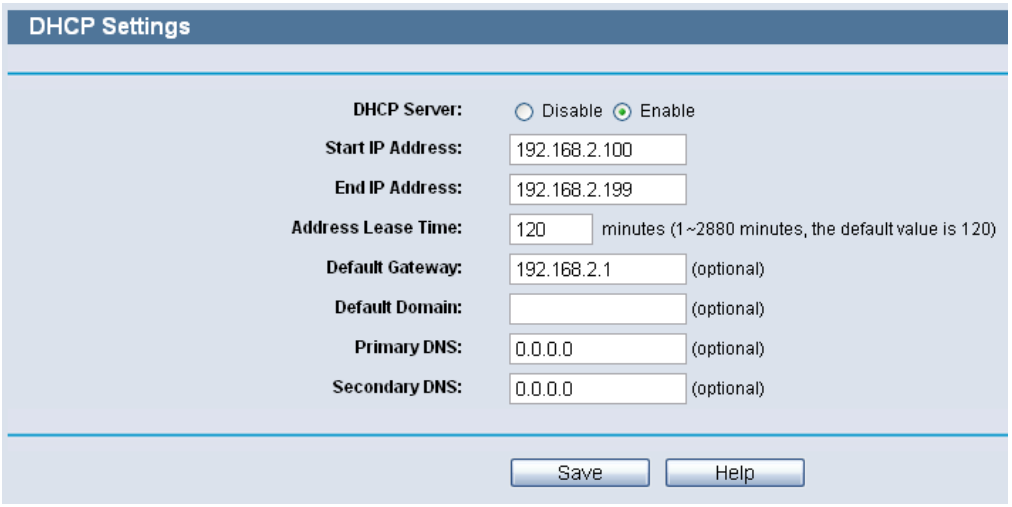
7 DHCP SETTINGS

There are three submenus under the DHCP menu: DHCP Settings, DHCP Clients List and Address Reservation. Click any of them, and you will be able to configure the corresponding function.

DHCP SETTINGS

Choose menu "DHCP->DHCP Settings", you can configure the DHCP Server on the page. The Router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PC(s) that are connected to the Router on the LAN.

Figure 56: DHCP Settings



- **DHCP Server** - Enable or Disable the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must configure the computer manually.
- **Start IP Address** - Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.2.100 is the default start address.
- **End IP Address** - Specify an IP address for the DHCP Server to end with when assigning IP addresses. 192.168.2.199 is the default end address.

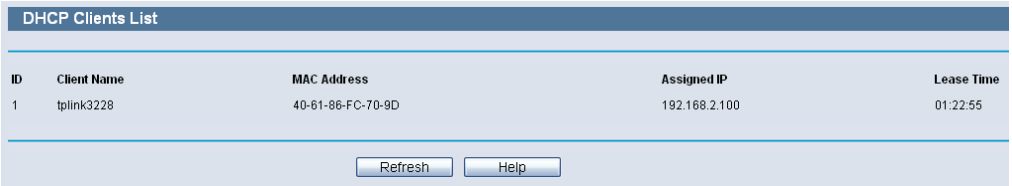
- **Address Lease Time** - The Address Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP Address. Enter the amount of time in minutes and the user will be "leased" this dynamic IP Address. After the time is up, the user will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.
- **Default Gateway** - (Optional.) Suggest to input the IP address of the LAN port of the Router, default value is 192.168.2.1
- **Default Domain** - (Optional.) Input the domain name of your network.
- **Primary DNS** - (Optional.) Input the DNS IP address provided by your ISP. Or consult your ISP.
- **Secondary DNS** - (Optional.) Input the IP address of another DNS server if your ISP provides two DNS servers.

NOTE: To use the DHCP server function of the Router, you must configure all computers on the LAN as "Obtain an IP Address automatically" mode.

DHCP CLIENTS LIST

Choose menu "DHCP->DHCP Clients List", you can view the information about the clients attached to the Router in the following screen.

Figure 57: DHCP Client List



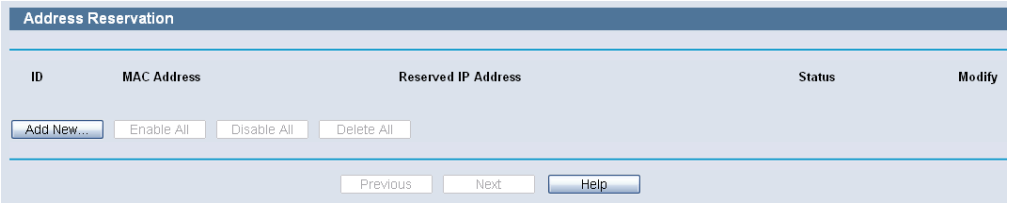
- **ID** - The index of the DHCP Client
- **Client Name** - The name of the DHCP client
- **MAC Address** - The MAC address of the DHCP client
- **Assigned IP** - The IP address that the Router has allocated to the DHCP client.
- **Lease Time** - The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP address will be automatically assigned to the user.

You cannot change any of the values on this page. To update this page and to show the current attached devices, click the Refresh button.

ADDRESS RESERVATION

Choose menu "DHCP->Address Reservation", you can view and add a reserved addresses for clients via the following figure.When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to the servers that require permanent IP settings.

Figure 58: Address Reservation

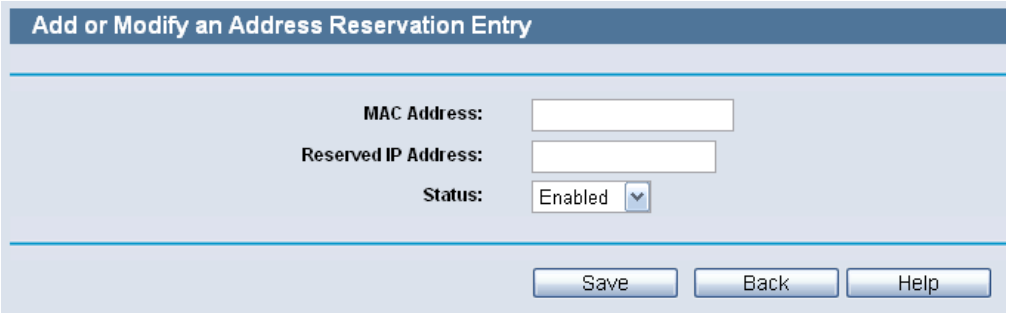


- **MAC Address** - The MAC address of the PC for which you want to reserve IP address.
- **Assigned IP Address** - The IP address of the Router reserved.
- **Status** - The status of this entry either Enabled or Disabled.

To Reserve IP addresses:

1. Click the Add New button.
2. Enter the MAC address (in XX-XX-XX-XX-XX-XX format.) and IP address in dotted-decimal notation of the computer you wish to add.
3. Click the Save button when finished.

Figure 59: Add or Modify an Address Reservation Entry



To modify or delete an existing entry:

1. Click the Modify in the entry you want to modify. If you want to delete the entry, click the Delete.

2. Modify the information.

3. Click the Save button.

Click the Enable/ Disabled All button to make all entries enabled/disabled

Click the Delete All button to delete all entries

Click the Next button to go to the next page and Click the Previous button to return the previous page.

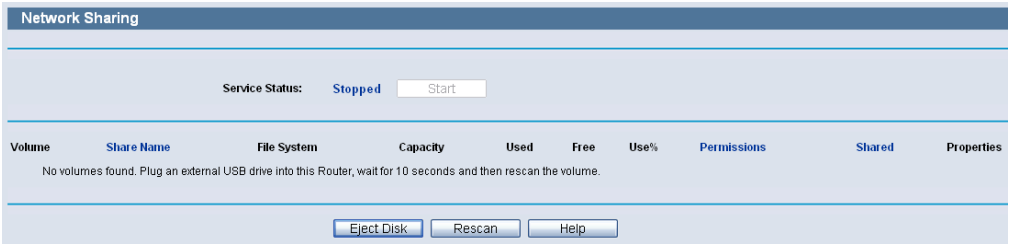
8 USB STORAGE SETTINGS

There are two submenus under the Network Sharing menu: Sharing Service and User Accounts. Click any of them, and you will be able to configure the corresponding function.

SHARING SERVICE

Choose menu "Network Sharing->Sharing Service", you can configure a USB disk drive attached to the Router on this page.

Figure 60: Network Sharing



- **Service Status** - Indicates the Network Sharing service's current status.
- **Volume** - The volume name of the USB drive the users have access to.
- **Share Name** - The specified share name of the volume.
- **File System** - The file system on the partition can be FAT32 or NTFS.
- **Capacity** - The storage capacity of the USB driver.
- **Used** - The used space of the USB driver.
- **Free** - The available space of the USB driver.
- **Use%** - The percentage of the used space.
- **Permissions** - Read-Only or Read/Write access to the volume designated as the share.
- **Shared** - Indicates the shared or non-shared status of the volume.
- **Properties** - Displays the Edit link to specify a volume that the Network Sharing users can access.

Click the Start button to start the Network Sharing service.

Click the Stop button to stop the Network Sharing service.

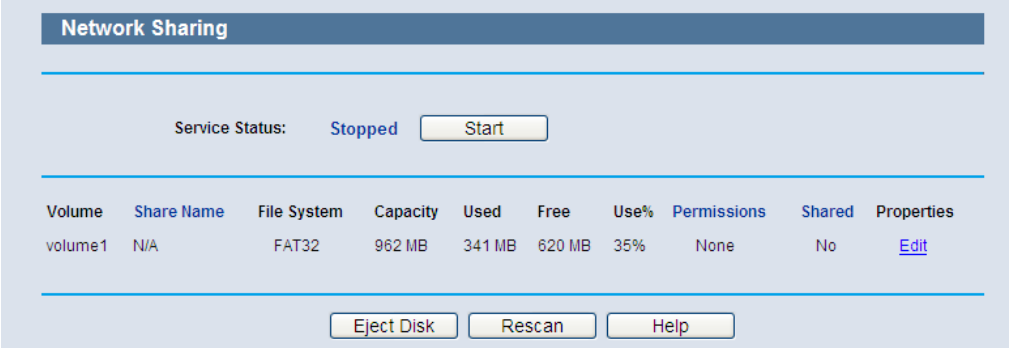
Click the Eject Disk button to safely remove the USB storage device that is connected to USB port. This takes the drive offline. A message will appear on your web browser when it is safe to detach the USB disk.

Click the Rescan button to start a new scan.

Follow the instructions below to set up your Router as a file server:

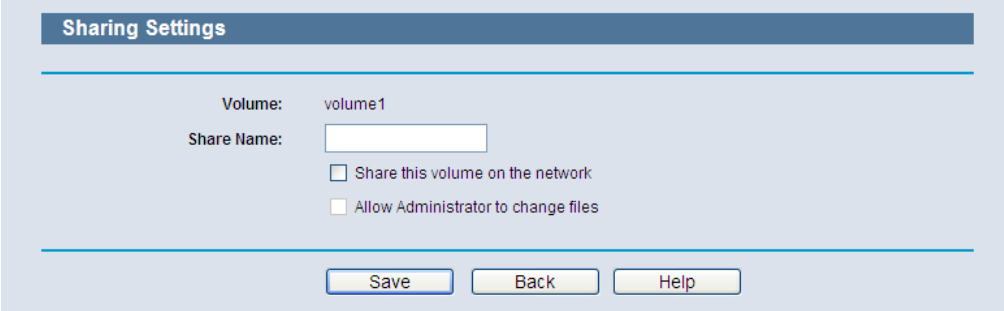
1. Plug an external USB hard disk drive or USB flash drive into this Router.
2. Click the Rescan button to find the USB drive that has been attached to the Router, and then the screen will appear as the following figure shown.

Figure 61: Sharing Settings - Rescan



3. To specify a volume that the Network Sharing users can access, click the Edit link in the Properties column and configure the share settings.
4. Set the Network Sharing user's username and password on User Accounts page.
5. Click the Start button to start the Network Sharing service.
6. Now the Network Sharing users inside your local network can access files on the USB drive from Internet Explorer at its Share Name followed by the Router's LAN IP address, for example: \\192.168.2.1\MyShare.

Figure 62: Sharing Settings - Edit



NOTE: The Router cannot automatically locate new USB drive. You have to click the Rescan button manually to display a list of volumes and information about them.

NOTE: The new settings will not take effect until you restart the service.

NOTE: To unplug the USB drive, click Eject Disk button first. Simply pulling USB drive out of the USB port can cause damage to the device and loss of data.

NOTE: Mounted volumes are subject to the 8-volume limit. So you cannot access more than 8 volumes on the USB storage device.

NOTE: NTFS is the recommended file system for Network Sharing because it supports several features that the other file systems do not, such as large files and large volume support.

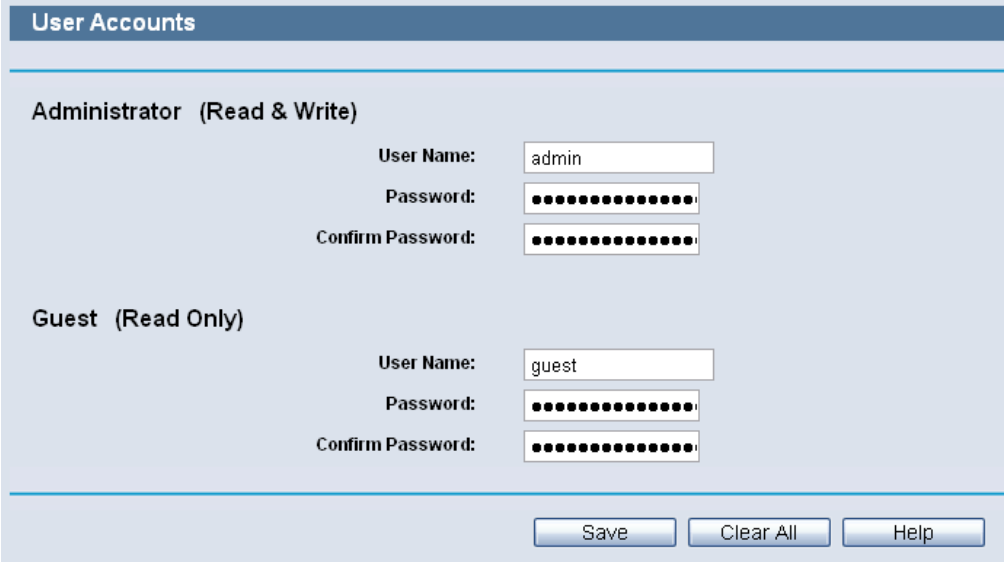
USER ACCOUNTS

You can specify the user name and password for Network Sharing users on the following User Accounts page. Network Sharing users can use Internet Explorer to access files on the USB drive.

There are two Network Sharing users that can access the shares. They are Administrator and Guest. Administrator has read/write access while Guest has read-only access.

Only Administrator can use a Web browser to transfer the files from a PC to the Writable shared volume on the USB drive.

Figure 63: User Accounts



- **User Name** - Type the user name that you want to give access to the USB drive. The user name must be composed of alphanumeric symbols not exceeding 15 characters in length.
- **Password** - Enter the password in the Password field. The password must be composed of alphanumeric symbols not exceeding 15 characters in length. For security purposes, the password for each user account is not displayed.
- **Confirm Password** - Re-enter the password here.

Click the Save button to save your settings.

Click the Clear All button to clear all the fields.

NOTE: 1. Please restart the service for the new settings to take effect.

2. If you cannot use the new user name and password to access the shares, press Windows logo + R to open the Run dialog box and type net use \\192.168.2.1 /delete /yes and press Enter. (192.168.2.1 is your Router's LAN IP address.)

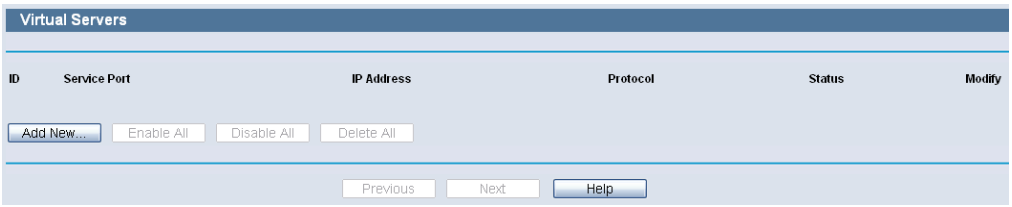
9 SPECIAL APPLICATION SETTINGS

There are four submenus under the Special Application menu: Virtual Servers, Port Triggering, DMZ and UPnP. Click any of them, and you will be able to configure the corresponding function.

VIRTUAL SERVERS

Choose menu "Special Application->Virtual Servers", you can view and add virtual servers in the following screen. Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP Address because its IP Address may be changed when using the DHCP function.

Figure 64: Virtual Servers Settings

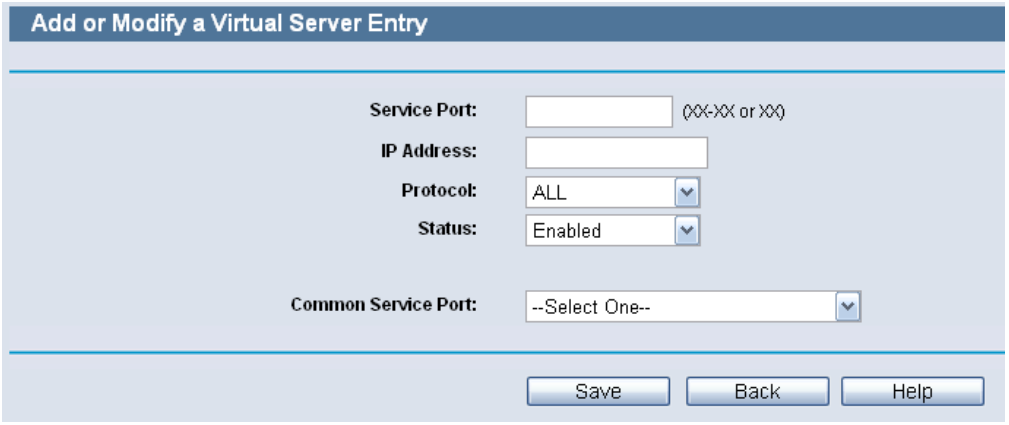


- **Service Port** - The numbers of External Ports. You can type a service port or a range of service ports (in XXX – YYY format, XXX is the start port number, YYY is the end port number).
- **IP Address** - The IP Address of the PC providing the service application.
- **Protocol** - The protocol used for this application, either TCP, UDP, or All (all protocols supported by the Router).
- **Status** - The status of this entry either Enabled or Disabled.

To setup a virtual server entry:

1. Click the Add New button.
2. Select the service you want to use from the Common Service Port list. If the Common Service Port list does not have the service that you want to use, type the number of the service port or service port range in the Service Port box.
3. Type the IP Address of the computer in the IP Address box.
4. Select the protocol used for this application, either TCP or UDP, or All.
5. Select the Enable check box to enable the virtual server.
6. Click the Save button.

Figure 65: Add or Modify a Virtual Server Entry



NOTE: If your computer or server has more than one type of available service, please select another service, and enter the same IP Address for that computer or server.

To modify or delete an existing entry:

1. Click the Modify in the entry you want to modify. If you want to delete the entry, click the Delete.
2. Modify the information.
3. Click the Save button.

Click the Enable/ Disabled All button to make all entries enabled/ disabled.

Click the Delete All button to delete all entries.

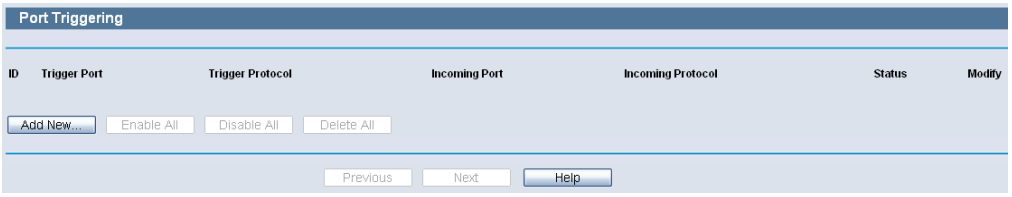
Click the Next button to go to the next page and click the Previous button to return the previous page.

NOTE: If you set the service port of the virtual server as 80, you must set the Web management port on System Tools –> Remote Management page to be any other value except 80 such as 8080. Otherwise there will be a conflict to disable the virtual server.

PORT TRIGGERING

Choose menu "Special Application->Port Triggering", you can view and add port triggering in the following screen. Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT Router. Port Triggering is used for some of these applications that can work with an NAT Router.

Figure 66: Port Triggering



Once the Router is configured, the operation is as follows:

1. A local host makes an outgoing connection using a destination port number defined in the Trigger Port field.
2. The Router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.
3. When necessary the external host will be able to connect to the local host using one of the ports defined in the Incoming Ports field.

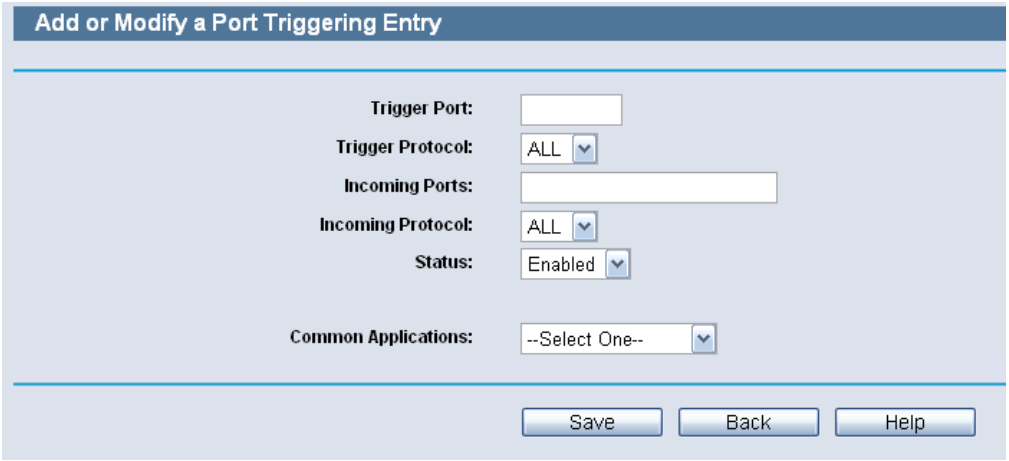
- **Trigger Port** - The port for outgoing traffic. An outgoing connection using this port will "Trigger" this rule.
- **Trigger Protocol** - The protocol used for Trigger Ports, either TCP, UDP, or All (all protocols supported by the Router).
- **Incoming Ports Range** - The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC that triggered this rule. You can input at most 5 groups of ports (or port section). Every group of ports must be set apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.
- **Incoming Protocol** - The protocol used for Incoming Ports Range, either TCP or UDP, or ALL (all protocols supported by the Router).

- **Status** - The status of this entry either Enabled or Disabled.

To add a new rule, follow the steps below.

1. Click the Add New button.
2. Select a common application from the Common Applications drop-down list, then the Trigger Port field and the Incoming Ports field will be automatically filled. If the Common Applications do not have the application you need, enter the Trigger Port and the Incoming Ports manually.
3. Select the protocol used for Trigger Port from the Trigger Protocol drop-down list, either TCP, UDP, or All.
4. Select the protocol used for Incoming Ports from the Incoming Protocol drop-down list, either TCP or UDP, or All.
5. Select Enable in Status field.
6. Click the Save button to save the new rule.

Figure 67: Add or Modify a Triggering Entry



To modify or delete an existing entry:

1. Click the Modify in the entry you want to modify. If you want to delete the entry, click the Delete.
2. Modify the information.
3. Click the Save button.

Click the Enable All button to make all entries enabled

Click the Disabled All button to make all entries disabled.

Click the Delete All button to delete all entries

NOTE: 1. When the trigger connection is released, the according opening ports will be closed.

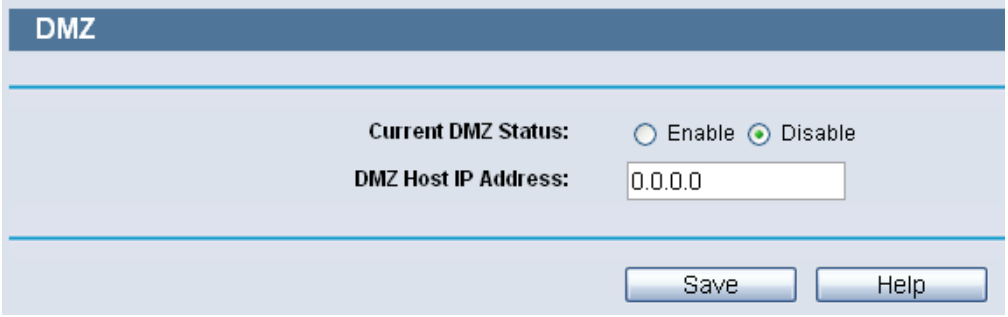
2. Each rule allowed to be used only by one host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.

3. Incoming Port Range cannot overlap each other.

DMZ

Choose menu "Special Application->DMZ", you can view and configure DMZ host in the screen. The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may be changed when using the DHCP function.

Figure 68: DMZ Settings



To assign a computer or server to be a DMZ server:

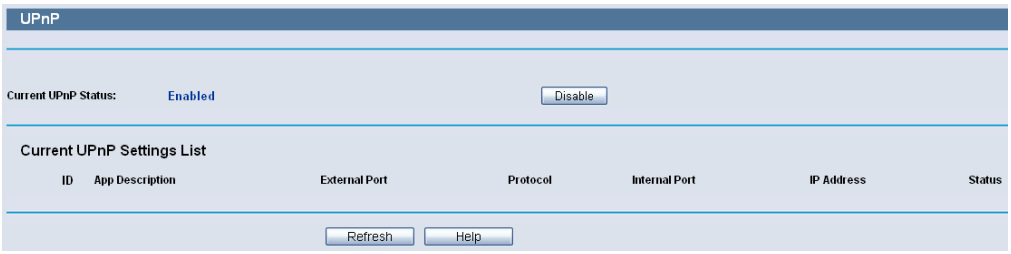
1. Click the Enable radio button
2. Enter the local host IP Address in the DMZ Host IP Address field
3. Click the Save button.

NOTE: After you set the DMZ host, the firewall related to the host will not work.

UPnP

Choose menu "Special Application->UPnP", you can view the information about UPnP(Universal Plug and Play) in the screen. The UPnP feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.

Figure 69: UPnP Settings



- **Current UPnP Status** - UPnP can be enabled or disabled by clicking the Enable or Disable button. As allowing this may present a risk to security, this feature is enabled by default.
- **Current UPnP Settings List** - This table displays the current UPnP information.
  - App Description -The description provided by the application in the UPnP request
  - External Port - External port, which the router opened for the application.
  - Protocol - Shows which type of protocol is opened.
  - Internal Port - Internal port, which the router opened for local host.
  - IP Address - The UPnP device that is currently accessing the router.
  - Status - The port's status displayed here. "Enabled" means that port is still active. Otherwise, the port is inactive.

Click Refresh to update the Current UPnP Settings List.

10 SECURITY SETTINGS

There are two submenus under the Security menu: Basic Security, and Advanced Security. Click any of them, and you will be able to configure the corresponding function.

BASIC SECURITY

Choose menu "Security->Basic Security", you can configure the basic security in the following screen.

Figure 70: Basic Security Settings

- **Firewall** - A firewall protects your network from the outside world. Here you can enable or disable the Router's firewall.
  - SPI Firewall - SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. SPI Firewall is enabled by

factory default. If you want all the computers on the LAN exposed to the outside world, you can disable it.

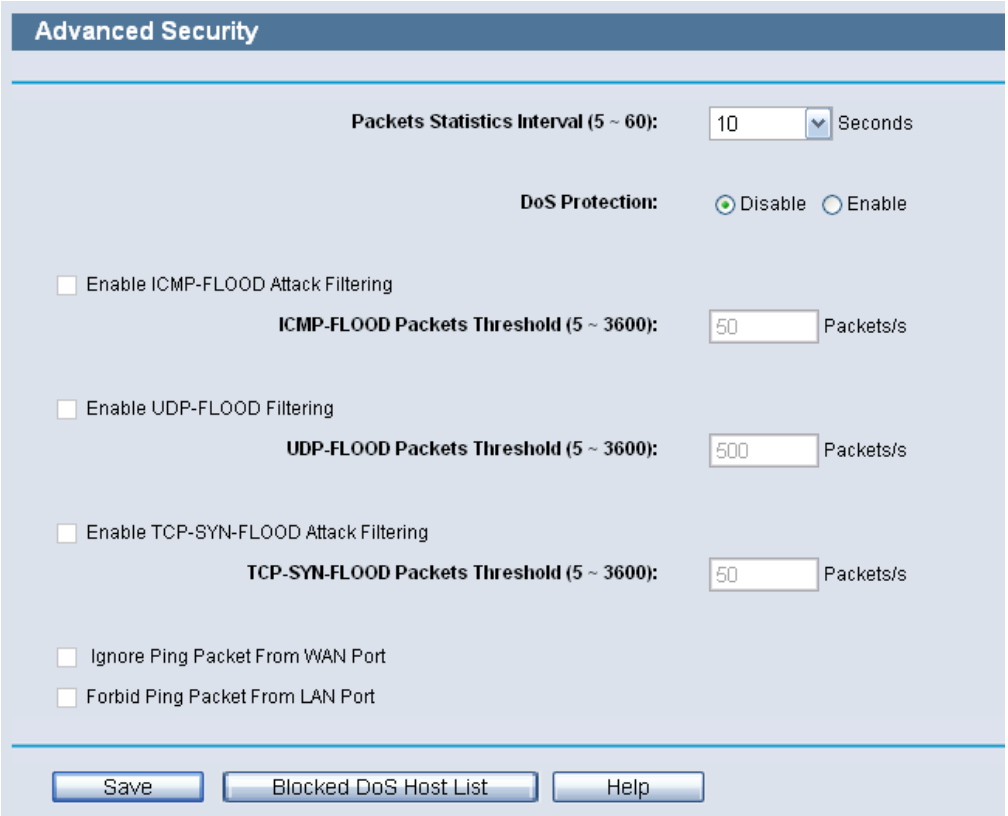
- **VPN** - VPN Passthrough must be enabled if you want to allow VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Router's firewall.
  - PPTP Passthrough - Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, keep the default, Enabled.
  - L2TP Passthrough - Layer 2 Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, keep the default, Enabled.
  - IPSec Passthrough - Internet Protocol Security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the Router, keep the default, Enabled.
- **ALG** - It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.
  - FTP ALG - To allow FTP clients and servers to transfer data across NAT, keep the default Enable.
  - TFTP ALG - To allow TFTP clients and servers to transfer data across NAT, keep the default Enable.
  - H323 ALG - To allow Microsoft NetMeeting clients to communicate across NAT, keep the default Enable.

Click the Save button to save your settings.

ADVANCED SECURITY

Choose menu "Security->Advanced Security", you can protect the Router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood in the following screen.

Figure 71: Advanced Security Settings



- **Packets Statistics Interval (5~60)** - The default value is 10. Select a value between 5 and 60 seconds from the drop-down list. The Packets Statistics Interval value indicates the time section of the packets statistics. The result of the statistics is used for analysis by SYN Flood, UDP Flood and ICMP-Flood.
- **DoS Protection** - Denial of Service protection. Check the Enable or Disable button to enable or disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.

NOTE: Dos Protection will take effect only when the Traffic Statistics in "System Tool->Traffic Statistics" is enabled.

- **Enable ICMP-FLOOD Attack Filtering** - Enable or Disable the ICMP-FLOOD Attack Filtering.

- **ICMP-FLOOD Packets Threshold (5~3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the current ICMP-FLOOD Packets number is beyond the set value, the Router will startup the blocking function immediately.

- **Enable UDP-FLOOD Filtering** - Enable or Disable the UDP-FLOOD Filtering.

- **UDP-FLOOD Packets Threshold (5~3600)** - The default value is 500. Enter a value between 5 ~ 3600. When the current UPD-FLOOD Packets number is beyond the set value, the Router will startup the blocking function immediately.

- **Enable TCP-SYN-FLOOD Attack Filtering** - Enable or Disable the TCP-SYN-FLOOD Attack Filtering.

- **TCP-SYN-FLOOD Packets Threshold (5~3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the current TCP-SYN-FLOOD Packets numbers is beyond the set value, the Router will startup the blocking function immediately.

- **Ignore Ping Packet From WAN Port** - Enable or Disable Ignore Ping Packet From WAN Port. The default setting is disabled. If enabled, the ping packet from the Internet cannot access the Router.

- **Forbid Ping Packet From LAN Port** - Enable or Disable Forbid Ping Packet From LAN Port. The default setting is disabled. If enabled, the ping packet from LAN cannot access the Router. This function can be used to defend against some viruses.

Click the Save button to save the settings.

Click the Blocked DoS Host List button to display the DoS host table by blocking.

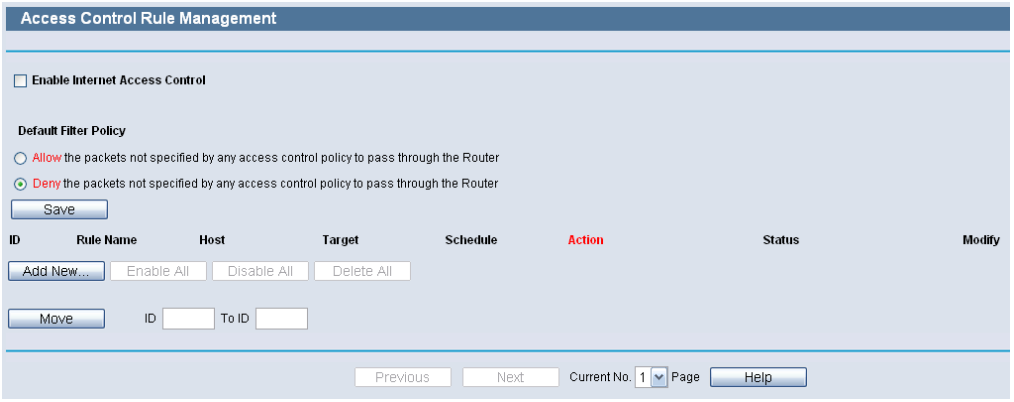
11 ACCESS CONTROL SETTINGS

There are five submenus under the Access Control menu: Rule, Host, Target, Schedule and Parental Control. Click any of them, and you will be able to configure the corresponding function.

RULE

Choose menu "Access Control->Rule", you can view and set Access Control rules in the screen as shown in the following.

Figure 72: Access Control Rule Management



- **Enable Internet Access Control** - Select the check box to enable the Internet Access Control function, so the Default Filter Policy can take effect.
- **Rule Name** - Here displays the name of the rule and this name is unique.
- **Host** - Here displays the host selected in the corresponding rule.
- **Target** - Here displays the target selected in the corresponding rule.
- **Schedule** - Here displays the schedule selected in the corresponding rule.
- **Action** - Here displays the action the Router takes to deal with the packets. It could be Allow or Deny. Allow means that the Router permits the packets to go through the Router. Deny means that the Router rejects the packets to go through the Router.

- **Status** - This field displays the status of the rule. Enabled means the rule will take effect, Disabled means the rule will not take effect.
- **Modify** - Here you can edit or delete an existing rule.

To add a new rule, please follow the steps below.

1. Click the Add New button and the next screen will pop-up.
2. Give a name (e.g. Rule_1) for the rule in the Rule Name field.
3. Select a host from the Host drop-down list or choose "Click Here To Add New Host List".
4. Select a target from the Target drop-sown list or choose "Click Here To Add New Target List".
5. Select a schedule from the Schedule drop-down list or choose "Click Here To Add New Schedule".
6. In the Action field, select Deny or Allow.
7. In the Status field, select Enabled or Disabled to enable or disable your entry.

Click the Save button.

Click the Enable All button to enable all the rules in the list.

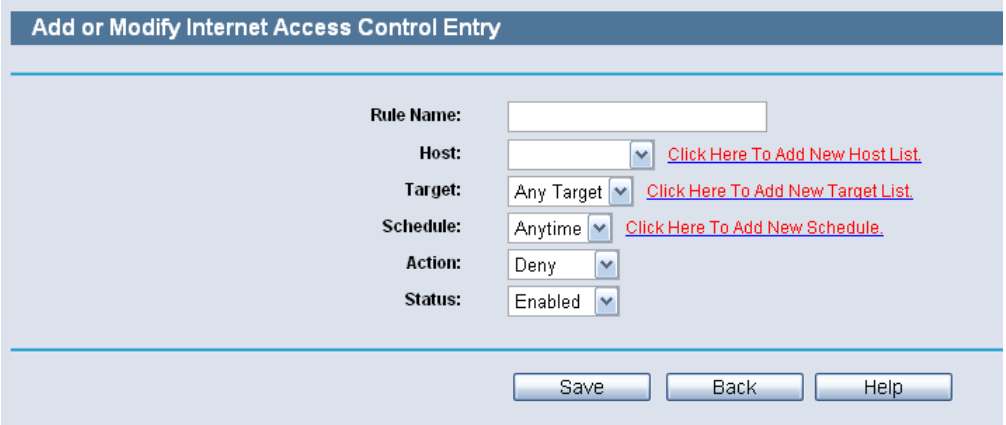
Click the Disable All button to disable all the rules in the list.

Click the Delete All button to delete all the entries in the table.

You can change the entry's order as desired. Fore entries are before hind entries. Enter the ID number in the first box you want to move and another ID number in second box you want to move to, and then click the Move button to change the entry's order.

Click the Next button to go to the next page, or click the Previous button return to the previous page.

Figure 73: Add or Modity Internet Access Control Entry



For example: If you desire to allow the host with MAC address 00-11-22-33-44-AA to access www.google.com only from 18:00 to 20:00 on Saturday and Sunday, and forbid other hosts in the LAN to access the Internet, you should follow the settings below:

1. Click "Access Control->Host" in the left to enter the Host Settings page. Add a new entry with the Host Description is Host_1 and MAC Address is 00-11-22-33-44-AA.

2. Click "Access Control->Target" in the left to enter the Target Settings page. Add a new entry with the Target Description is Target_1 and Domain Name is www.google.com.

3. Click "Access Control->Schedule" in the left to enter the Schedule Settings page. Add a new entry with the Schedule Description is Schedule_1, Day is Sat and Sun, Start Time is 1800 and Stop Time is 2000.

4. Click "Access Control->Rule" in the left to return to the Access Control Rule Management page. Select "Enable Internet Access Control" and choose "Deny the packets not specified by any access control policy to pass through the Router".

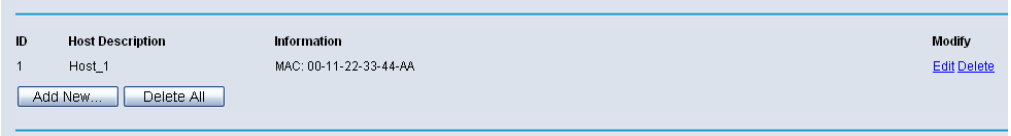
5. Click the Add New button to add a new rule as follows:

   - In Rule Name field, create a name for the rule. Note that this name should be unique, for example Rule_1.
   - In Host field, select Host_1.
   - In Target field, select Target_1.
   - In Schedule field, select Schedule_1.
   - In Action field, select Allow.
   - In Status field, select Enable.

- Click Save to complete the settings.

Then you will go back to the Access Control Rule Management page and see the following list.

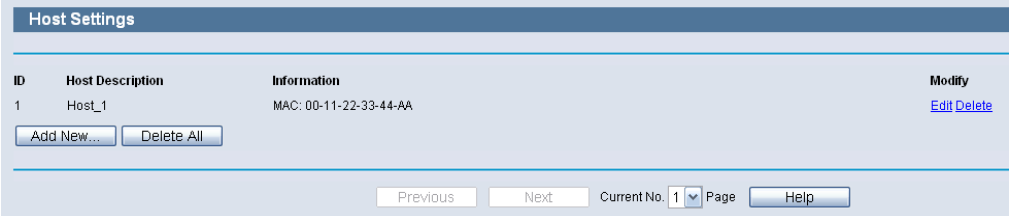
Figure 74: Display Access Control Entry



HOST

Choose menu "Access Control->Host", you can view and set a Host list in the following screen. The host list is necessary for the Access Control Rule.

Figure 75: Host Settings



- **Host Description** - Here displays the description of the host and this description is unique.
- **Information** - Here displays the information about the host. It can be IP or MAC.
- **Modify** - To modify or delete an existing entry.

To add a new entry, please follow the steps below.

1. Click the Add New button.
2. In the Mode field, select IP Address or MAC Address.
   - If you select IP Address, the screen shown is Figure 75.

     1) In Host Description field, create a unique description for the host (e.g. Host_1).

     2) In LAN IP Address field, enter the IP address.
   - If you select MAC Address, the screen shown is Figure 76.

     1) In Host Description field, create a unique description for the host (e.g. Host_1).

2) In MAC Address field, enter the MAC address.

3. Click the Save button to complete the settings.

Click the Delete All button to delete all the entries in the table.

Click the Next button to go to the next page, or click the Previous button return to the previous page.

Figure 76: Host Entry IP address Mode

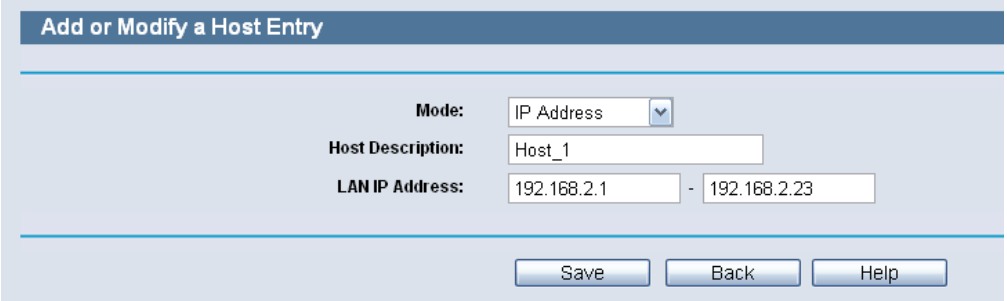
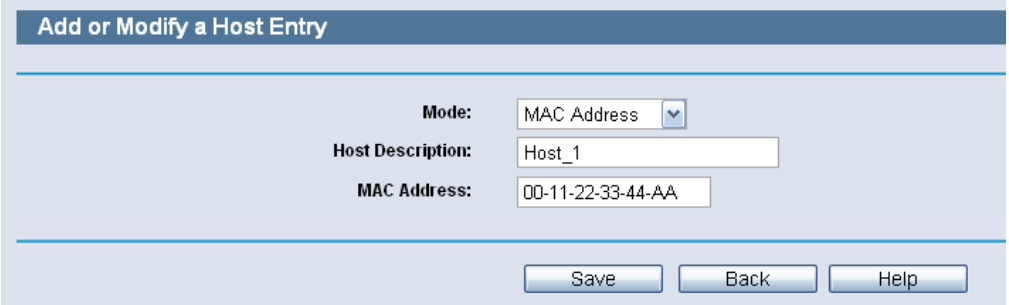


Figure 77: Host Entry MAC address Mode



For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA, you should first follow the settings below:

1. Click the Add New button.

2. In Mode field, select MAC Address from the drop-down list.

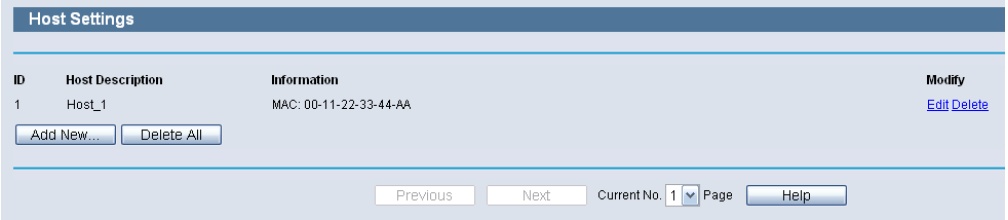
3. In Host Description field, create a unique description for the host (e.g. Host_1).

4. In MAC Address field, enter 00-11-22-33-44-AA.

5. Click Save to complete the settings.

Then you will go back to the Host Settings page and see the following list.

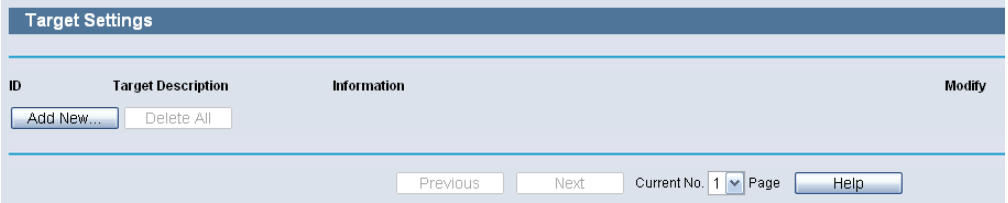
Figure 78: Host Settings



TARGET

Choose menu "Access Control->Target", you can view and set a Target list in the screen as shown in the following figure. The target list is necessary for the Access Control Rule.

Figure 79: Target Settings



- **Target Description** - Here displays the description about the target and this description is unique.
- **Information** - The target can be IP address, port, or domain name.
- **Modify** - To modify or delete an existing entry.

To add a new entry, please follow the steps below.

1. Click the Add New button.
2. In Mode field, select IP Address or Domain Name.
   - If you select IP Address, the screen shown is Figure 79.

     1) In Target Description field, create a unique description for the target (e.g. Target_1).

     2) In IP Address field, enter the IP address of the target.

     3) Select a common service from Common Service Port drop-down list, so that the Target Port will be automatically filled. If the Common Service Port drop-down list doesn't have the service you want, specify the Target Port manually.

     4) In Protocol field, select TCP, UDP, ICMP or ALL.

- If you select Domain Name, the screen shown is Figure 80.

  1) In Target Description field, create a unique description for the target (e.g. Target_1).

  2) In Domain Name field, enter the domain name, either the full name or the keywords (for example google) in the blank. Any domain name with keywords in it (www.google.com, www.google.cn) will be blocked or allowed. You can enter 4 domain names.

3. Click the Save button.

Click the Delete All button to delete all the entries in the table.

Click the Next button to go to the next page, or click the Previous button return to the previous page.

Figure 80: Target Settings-IP Address Mode

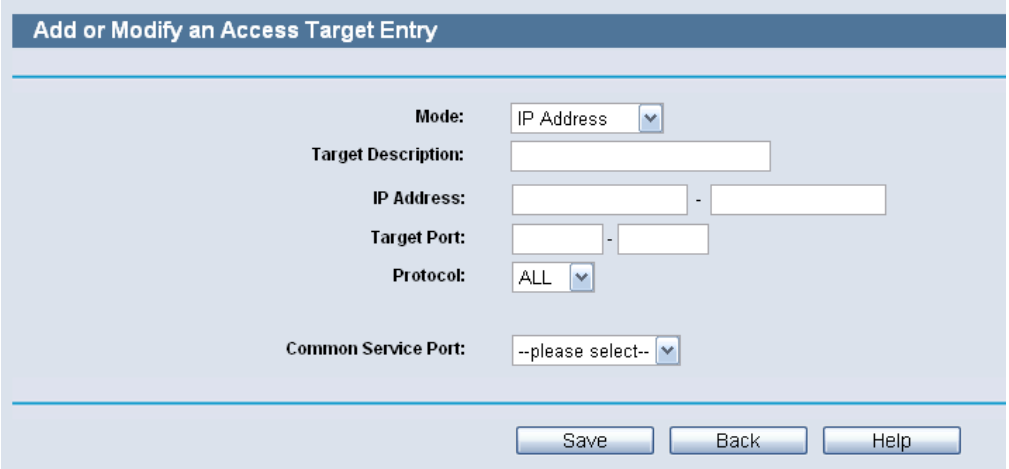
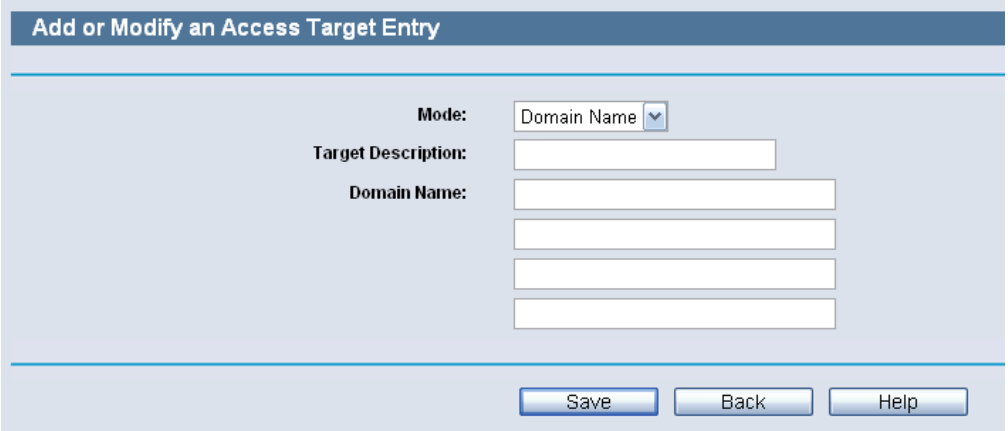


Figure 81: Target Settings-Domain Name Mode

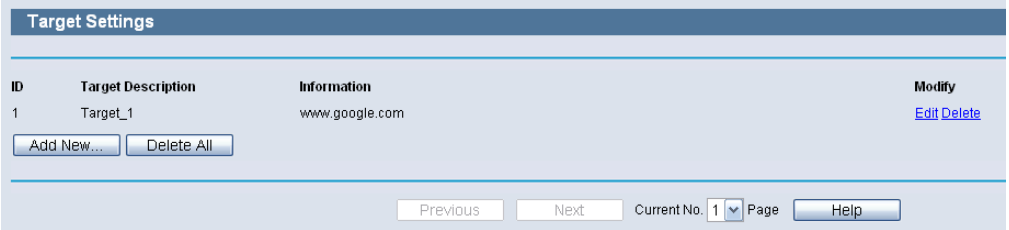


For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA in the LAN to access www.google.com only, you should first follow the settings below:

1. Click the Add New button.
2. In Mode field, select Domain Name from the drop-down list.
3. In Target Description field, create a unique description for the target (e.g. Target_1).
4. In Domain Name field, enter www.google.com.
5. Click Save to complete the settings.

Then you will go back to the Target Settings page and see the following list.

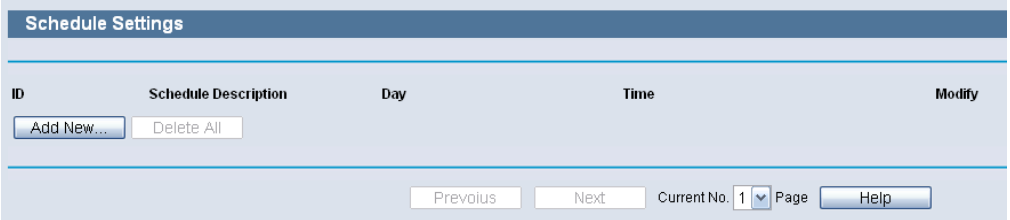
Figure 82: Target Settings-Domain Name Mode



SCHEDULE

Choose menu "Access Control->Schedule", you can view and set a Schedule list in the next screen as shown in the following figure. The Schedule list is necessary for the Access Control Rule.

Figure 83: Schedule Settings



- **Schedule Description** - Here displays the description of the schedule and this description is unique.
- **Day** - Here displays the day(s) in a week.
- **Time** - Here displays the time period in a day.
- **Modify** - Here you can edit or delete an existing schedule.

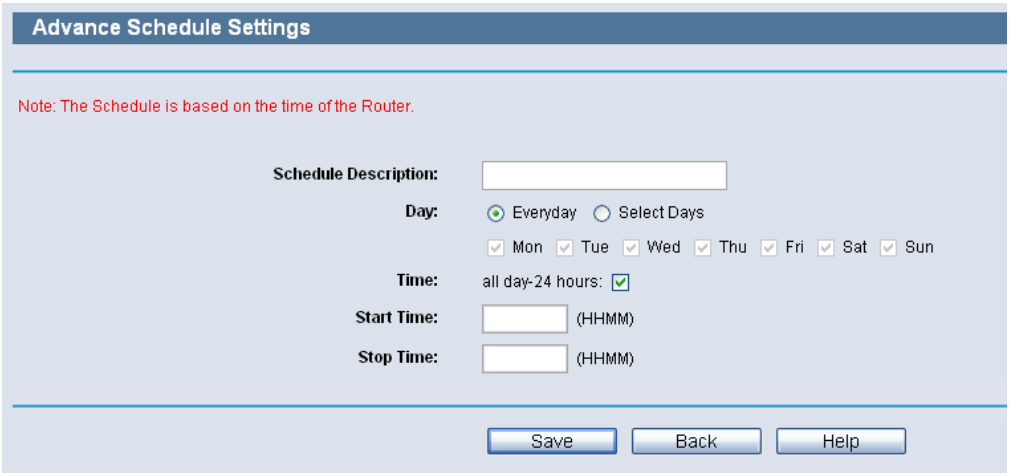
To add a new schedule, follow the steps below.

1. Click the Add New button shown in Figure 82 and the next screen will pop-up.
2. In Schedule Description field, create a unique description for the schedule (e.g. Schedule_1).
3. In Day field, select the day or days you need.
4. In Time field, you can select all day-24 hours or you may enter the Start Time and Stop Time in the corresponding field.
5. Click Save to complete the settings.

Click the Delete All button to delete all the entries in the table.

Click the Next button to go to the next page, or click the Previous button return to the previous page.

Figure 84: Advanced Schedule Settings



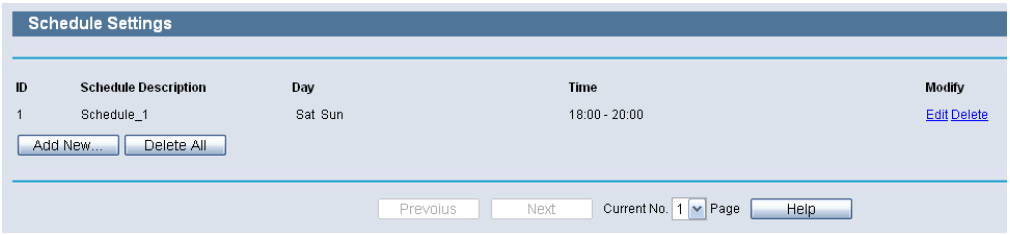
For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA to access www.google.com only from 18:00 to 20:00 on Saturday and Sunday, you should first follow the settings below:

1. Click the Add New button.
2. In Schedule Description field, create a unique description for the schedule (e.g. Schedule_1).
3. In Day field, check the Select Days radio button and then select Sat and Sun.
4. In Time field, enter 1800 in Start Time field and 2000 in Stop Time field.

5. Click Save to complete the settings.

Then you will go back to the Schedule Settings page and see the following list.

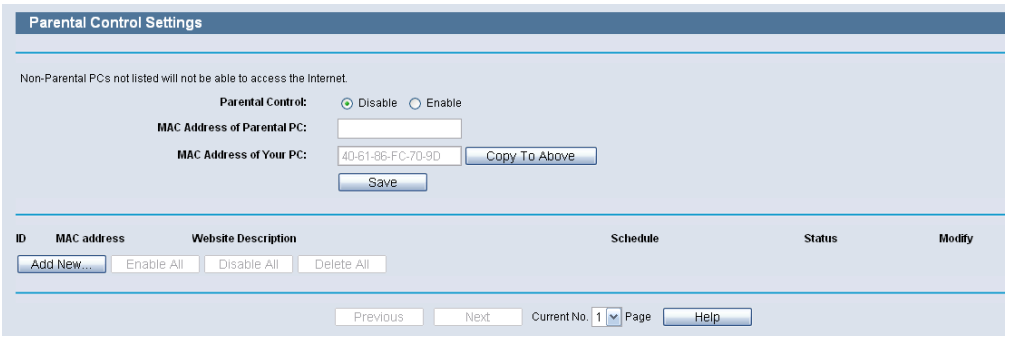
Figure 85: Advanced Schedule Settings



PARENTAL CONTROL

Choose menu "Parental Control", and you can configure the parental control in the screen as shown in the following figure. The Parental Control function can be used to control the internet activities of the child, limit the child to access certain websites and restrict the time of surfing.

Figure 86: Parental Control Settings



- **Parental Control** - Check Enable if you want this function to take effect, otherwise check Disable.
- **MAC Address of Parental PC** - In this field, enter the MAC address of the controlling PC, or you can make use of the Copy To Above button below.
- **MAC Address of Your PC** - This field displays the MAC address of the PC that is managing this Router. If the MAC Address of your adapter is registered, you can click the Copy To Above button to fill this address to the MAC Address of Parental PC field above.
- **Website Description** - Description of the allowed website for the PC controlled.

- **Schedule** - The time period allowed for the PC controlled to access the Internet. For detailed information, please go to "Access Control ? Schedule".

- **Modify** - Here you can edit or delete an existing entry.

To add a new entry, please follow the steps below.

1. Click the Add New button.

2. Enter the MAC address of the PC (e.g. 00-11-22-33-44-AA) you'd like to control in the MAC Address of Child PC field. Or you can choose the MAC address from the All Address in Current LAN drop-down list.

3. Give a description (e.g. Allow Google) for the website allowed to be accessed in the Website Description field.

4. Enter the allowed domain name of the website, either the full name or the keywords (e.g. google) in the Allowed Domain Name field. Any domain name with keywords in it (www.google.com.cn) will be allowed.

5. Select from the Effective Time drop-down list the schedule (e.g. Schedule_1) you want the entry to take effect. If there are not suitable schedules for you, click the Schedule in red below to go to the Advance Schedule Settings page and create the schedule you need.

6. In the Status field, you can select Enabled or Disabled to enable or disable your entry.

7. Click the Save button.

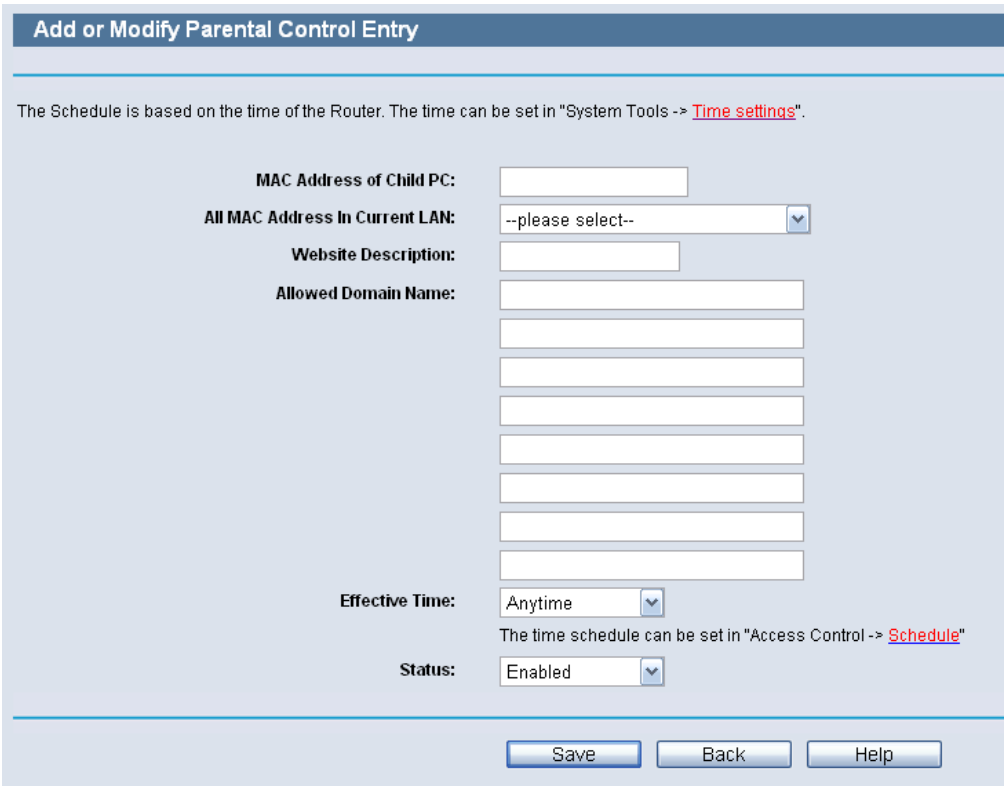
Click the Enable All button to enable all the rules in the list.

Click the Disable All button to disable all the rules in the list.

Click the Delete All button to delete all the entries in the table.

Click the Next button to go to the next page, or click the Previous button return to the previous page.

Figure 87: Add or Modify Parental Control Entry


Add or Modify Parental Control Entry
The Schedule is based on the time of the Router. The time can be set in "System Tools -> Time settings".
MAC Address of Child PC:
All MAC Address In Current LAN:
--please select--
Website Description:
Allowed Domain Name:
Effective Time:
Anytime
The time schedule can be set in "Access Control -> Schedule"
Status:
Enabled
Save
Back
Help

For example: If you desire that the child PC with MAC address 00-11-22-33-44-AA can access www.google.com on Saturday only while the parent PC with MAC address 00-11-22-33-44-BB is without any restriction, you should follow the settings below.

1. Click "Parental Control" menu on the left to enter the Parental Control Settings page. Check Enable and enter the MAC address 00-11-22-33-44-BB in the MAC Address of Parental PC field.

2. Click "Access Control->Schedule" on the left to enter the Schedule Settings page. Clickthe Add New button to create a new schedule with Schedule Description is Schedule_1, Day is Sat and Time is all day-24 hours.

3. Click "Parental Control" menu on the left to go back to the Add or Modify Parental Control Entry page:

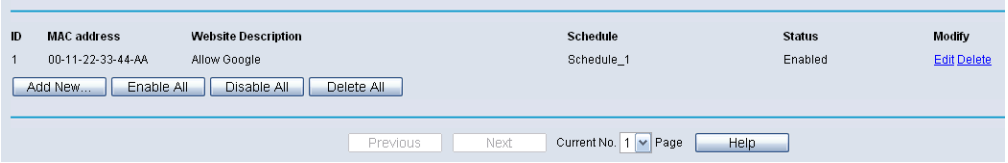
   - Click the Add New button.
   - Enter 00-11-22-33-44-AA in the MAC Address of Child PC field.
   - Enter "Allow Google" in the Website Description field.
   - Enter "www.google.com" in the Allowed Domain Name field.

- Select “Schedule_1” you create just now from the Effective Time drop-down list.
- In Status field, select Enable.

4. Click Save to complete the settings.

Then you will go back to the Parental Control Settings page and see the following list, as shown in the following figure.

Figure 88: Parental Control Settings

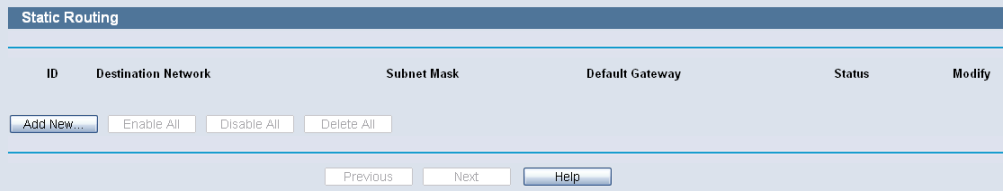


12 ADVANCED ROUTING

STATIC ROUTING LIST

Choose menu "Advanced Routing", you can configure the static route in the next screen. A static route is a pre-determined path that network information must travel to reach a specific host or network.

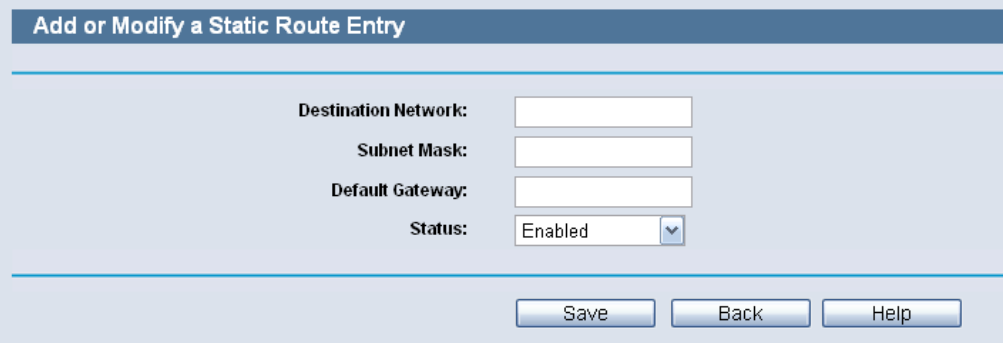
Figure 89: Static Routing



To add static routing entries:

1. Click the Add New button.

Figure 90: Add or Modify a Static Route Entry



2. Enter the following data:

- **Destination IP Address** - The Destination IP Address is the address of the network or host that you want to assign to a static route.
- **Subnet Mask** - The Subnet Mask determines which portion of an IP Address is the network portion, and which portion is the host portion.
- **Gateway** - This is the IP Address of the gateway device that allows for contact between the Router and the network or host.

3. Select Enabled or Disabled for this entry on the Status pull-down list.

4. Click the Save button to make the entry take effect.

Other configurations for the entries:

Click the Delete button to delete the entry.

Click the Enable All button to enable all the entries.

Click the Disable All button to disable all the entries.

Click the Delete All button to delete all the entries.

Click the Previous button to view the information in the previous screen, click the Next button to view the information in the next screen.

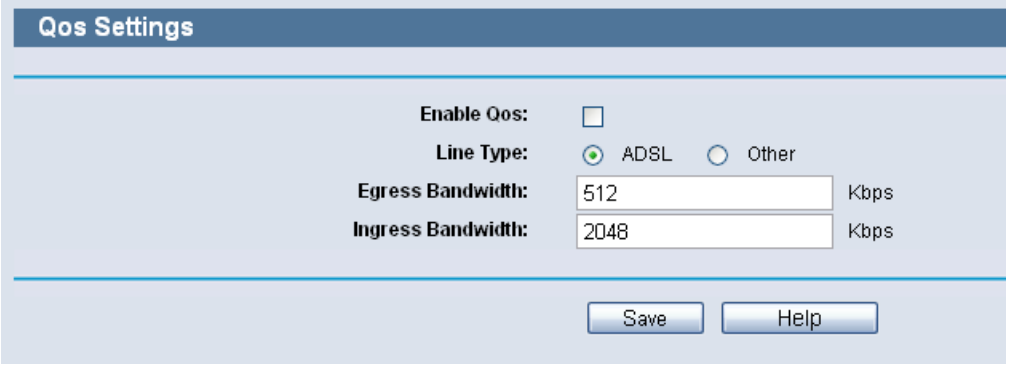
13 QoS Settings

There are two submenus under the QoS menu: QoS Settings and Rules List. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

QoS Settings

Choose menu "QoS->QoS Settings", you can configure the Egress Bandwidth and Ingress Bandwidth in the next screen. Their values you configure should be less than 100000Kbps. For optimal control of the bandwidth, please select the right Line Type and ask your ISP for the total bandwidth of the egress and ingress.

Figure 91: QoS Settings

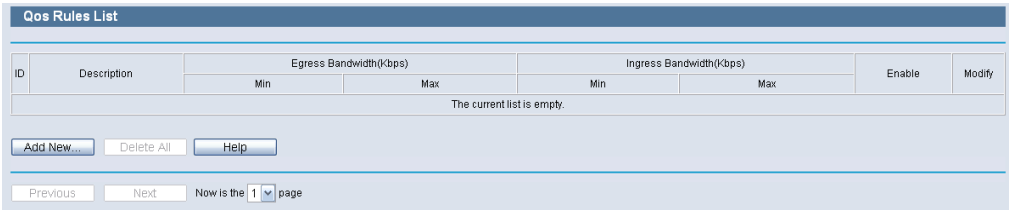


- **Enable QoS** - Check this box so that the QoS settings can take effect.
- **Line Type** - Select the right type for you network connection. If you don't know how to choose, please ask your ISP for the information.
- **Egress Bandwidth** - The upload speed through the WAN port.
- **Ingress Bandwidth** - The download speed through the WAN port.

RULES LIST

Choose menu "QoS->Rules List", you can view and configure the QoS rules in the screen below.

Figure 92: QoS Rules List

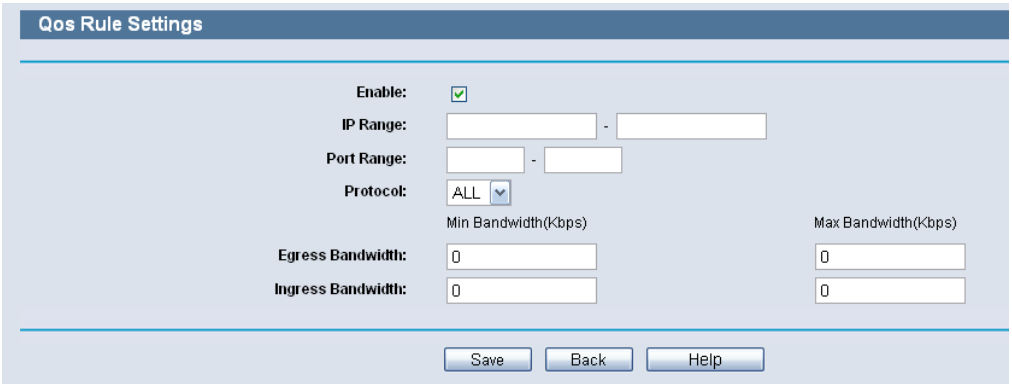


- **Description** - This is the information about the rules such as address range.
- **Egress bandwidth** - This field displays the max and mix upload bandwidth through the WAN port, the default is 0.
- **Ingress bandwidth** - This field displays the max and mix download bandwidth through the WAN port, the default is 0.
- **Enable** - This displays the status of the rule.
- **Modify** - Click Modify to edit the rule. Click Delete to delete the rule.

To add/modify a QoS rule, follow the steps below.

1. Click the Add New buttonshown in Figure 91, you will see a new screen shown in Figure 92.
2. Enter the information like the screen shown below.
3. Click the Save button.

Figure 93: QoS Rule Settings



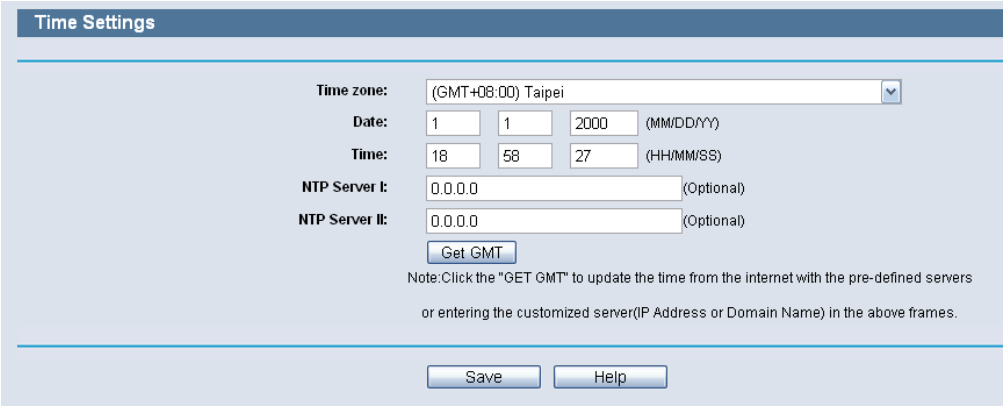
14 SYSTEM TOOLS

Choose menu “System Tools”, and you can see the submenus under the main menu: Time Settings, Diagnostic, Setting Management, Password, System Log, Statistics, Local Management and Remote Management. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

TIME SETTING

Choose menu “System Tools->Time Setting”, you can configure the time on the following screen.

Figure 94: Time Settings



- **Time Zone** - Select your local time zone from this pull down list.
- **Date** - Enter your local date in MM/DD/YY into the right blanks.
- **Time** - Enter your local time in HH/MM/SS into the right blanks.
- **NTP Server Prior** - Enter the address for the NTP Server, then the Router will get the time from the NTP Server preferentially. In addition, the Router built-in some common NTP Servers, so it can get time automatically once it connects the Internet.

To configure the system manually:

1. Select your local time zone.
2. Enter date and time in the right blanks.

3. Click Save to save the configuration.

To configure the system automatically:

1. Select your local time zone.
2. Enter the IP address for NTP Server Prior.
3. Click the Get GMT button to get system time from Internet if you have connected to the Internet.

NOTE: This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully, otherwise, these functions will not take effect.

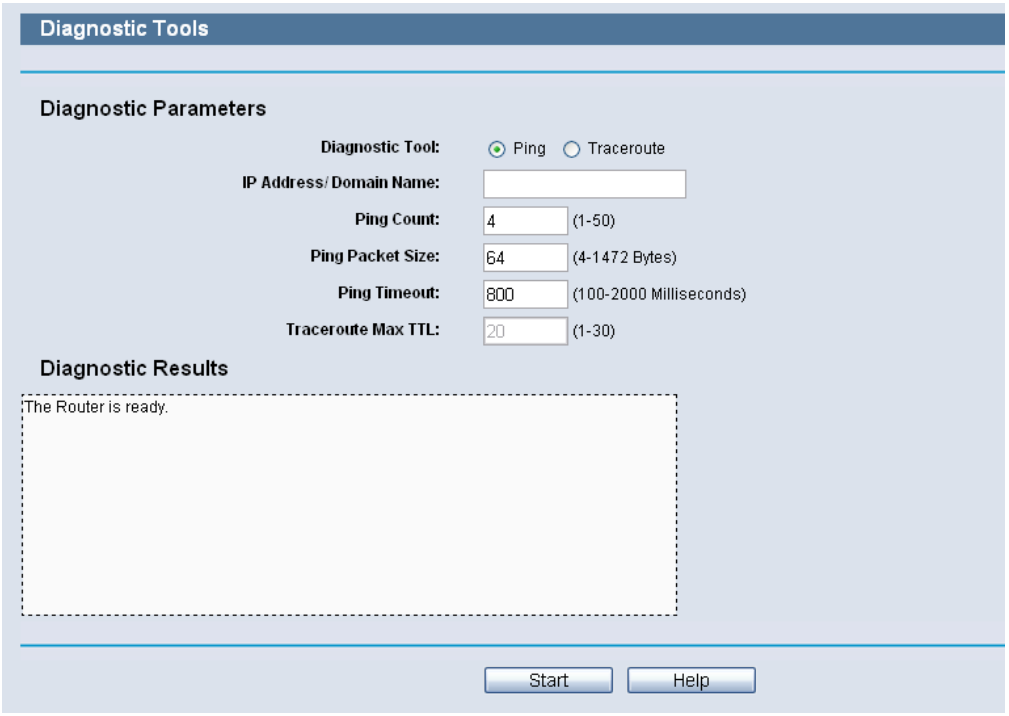
NOTE: The time will be lost if the router is turned off.

NOTE: The router will obtain GMT automatically from Internet if it has already connected to Internet.

DIAGNOSTIC

Choose menu "System Tools->Diagnostic", you can transact Ping or Traceroute function to check connectivity of your network in the following screen.

Figure 95: Diagnostic Tools



- **Diagnostic Tool** - Check the radio button to select one diagnostic too.
  - **Ping** - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
  - **Traceroute** - This diagnostic tool tests the performance of a connection.

NOTE: You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

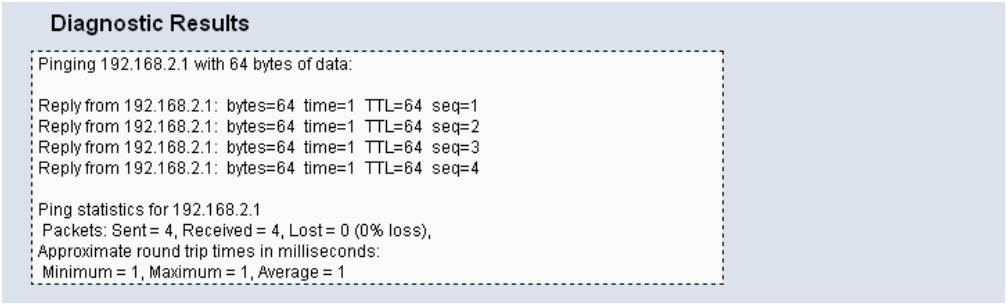
- **IP Address/Domain Name** - Type the destination IP address (such as 202.108.22.5) or Domain name (such as http://www.smc.com)
- **Pings Count** - The number of Ping packets for a Ping connection.
- **Ping Packet Size** - The size of Ping packet.
- **Ping Timeout** - Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime.
- **Traceroute Max TTL** - The max number of hops for a Traceroute connection.

Click Start to check the connectivity of the Internet.

The Diagnostic Results page displays the result of diagnosis.

If the result is similar to the following screen, the connectivity of the Internet is fine.

Figure 96: Diagnostic Results


Diagnostic Results
Pinging 192.168.2.1 with 64 bytes of data:
Reply from 192.168.2.1: bytes=64 time=1 TTL=64 seq=1
Reply from 192.168.2.1: bytes=64 time=1 TTL=64 seq=2
Reply from 192.168.2.1: bytes=64 time=1 TTL=64 seq=3
Reply from 192.168.2.1: bytes=64 time=1 TTL=64 seq=4
Ping statistics for 192.168.2.1
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
Minimum = 1, Maximum = 1, Average = 1

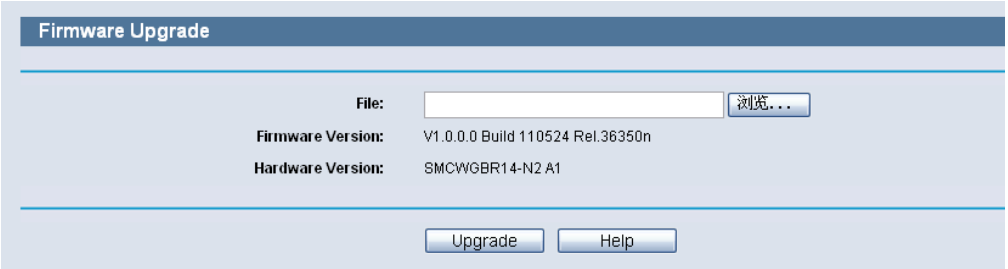
NOTE: Only one user can use this tool at one time. Options "Number of Pings", "Ping Size" and "Ping Timeout" are used for Ping function. Option "Tracert Hops" are used for Tracert function.

SETTINGS MANAGEMENT

FIRMWARE UPGRADE

Choose menu "System Tools->Firmware Upgrade", you can update the latest version of firmware for the Router on the following screen.

Figure 97: Firmware Upgrade



- **Firmware Version** - This displays the current firmware version.
- **Hardware Version** - This displays the current hardware version. The hardware version of the upgrade file must accord with the Router's current hardware version.

To upgrade the Router's firmware, follow these instructions below:

1. Download a more recent firmware upgrade file from the SMC website (http://www.smc.com).
2. Type the path and file name of the update file into the File field. Or click the Browse button to locate the update file.
3. Click the Upgrade button.

NOTE: New firmware versions are posted at http://www.smc.com and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the Router rather than the configuration, you can try to upgrade the firmware.

NOTE: When you upgrade the Router's firmware, you may lose its current configurations, so before upgrading the firmware please write down some of your customized settings to avoid losing important settings.

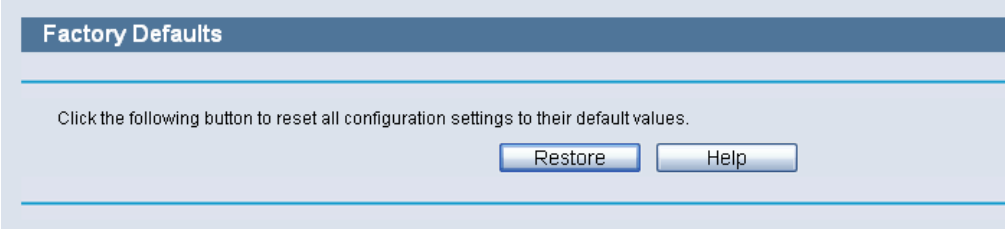
NOTE: Do not turn off the Router or press the Reset button while the firmware is being upgraded, otherwise, the Router may be damaged.

NOTE: The Router will reboot after the upgrading has been finished.

FACTORY DEFAULTS

Choose menu "System Tools-> Factory Defaults", and you can restore the configurations of the Router to factory defaults on the following screen.

Figure 98: Restore Factory Default


Factory Defaults
Click the following button to reset all configuration settings to their default values.
Restore
Help

Click the Restore button to reset all configuration settings to their default values.

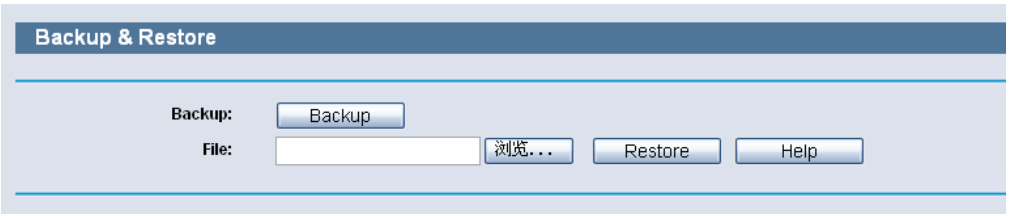
- The default User Name: admin
- The default Password: smcadmin
- The default IP Address: 192.168.2.1
- The default Subnet Mask: 255.255.255.0

NOTE: Any settings you have saved will be lost when the default settings are restored.

BACKUP & RESTORE

Choose menu "System Tools-> Backup & Restore", you can save the current configuration of the Router as a backup file and restore the configuration via a backup file as shown in the following figure.

Figure 99: Backup & Restore Configuration



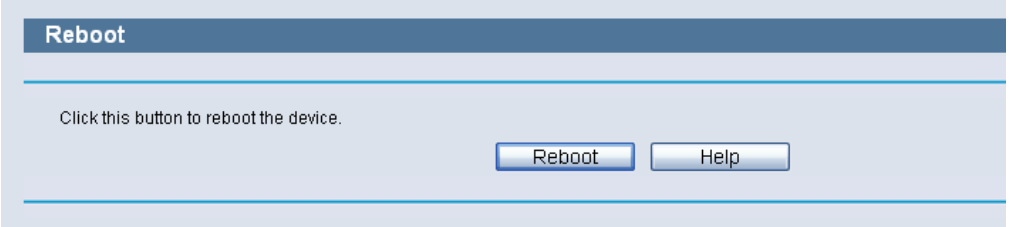
- Click the Backup button to save all configuration settings as a backup file in your local computer.
- To upgrade the Router's configuration, follow these instructions.
  - Click the Browse... button to locate the update file for the Router, or enter the exact path to the Setting file in the text box.
  - Click the Restore button.

NOTE: The current configuration will be covered by the uploading configuration file. The upgrade process lasts for 20 seconds and the Router will restart automatically. Keep the Router on during the upgrading process to prevent any damage.

REBOOT

Choose menu "System Tools->Reboot", you can click the Reboot button to reboot the Router via the next screen.

Figure 100: Reboot



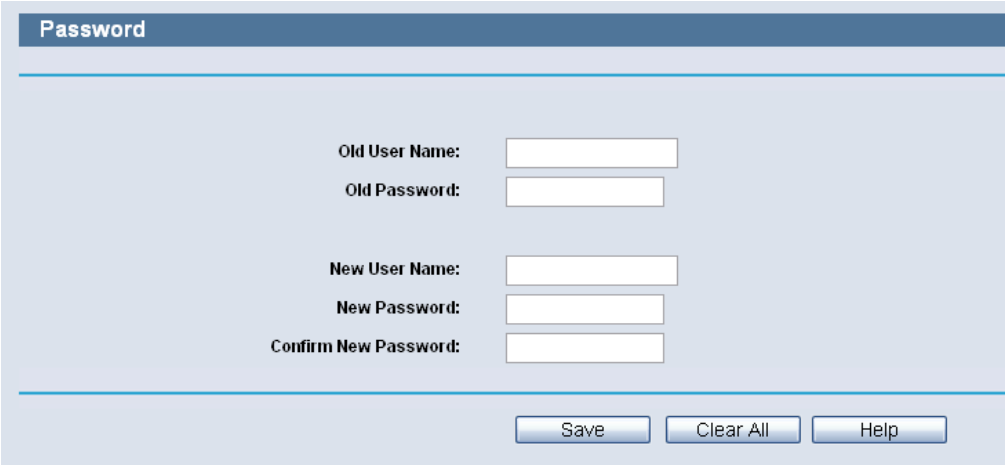
Some settings of the Router will take effect only after rebooting, which include

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Wireless configurations.
- Change the Web Management Port.
- Upgrade the firmware of the Router (system will reboot automatically).
- Restore the Router's settings to factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically.

PASSWORD

Choose menu “System Tools->Password”, you can change the factory default user name and password of the Router in the next screen as shown in the following figure.

Figure 101: Password



It is strongly recommended that you should change the factory default user name and password of the Router, because all users who try to access the Router's Web-based utility or Quick Setup will be prompted for the Router's default user name and password.

NOTE: The new user name and password must not exceed 14 characters in length and not include any spaces. Enter the new Password twice to confirm.

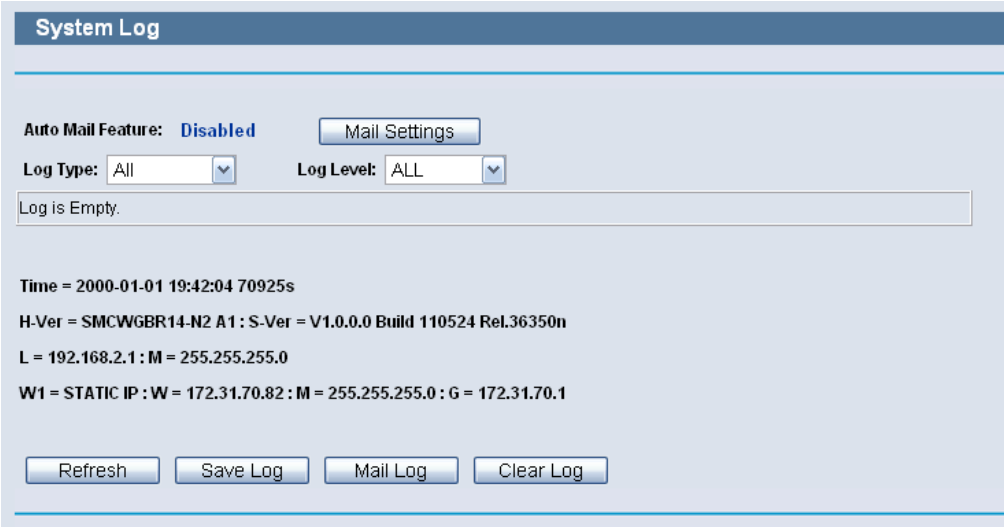
Click the Save button when finished.

Click the Clear All button to clear all.

SYSTEM LOG

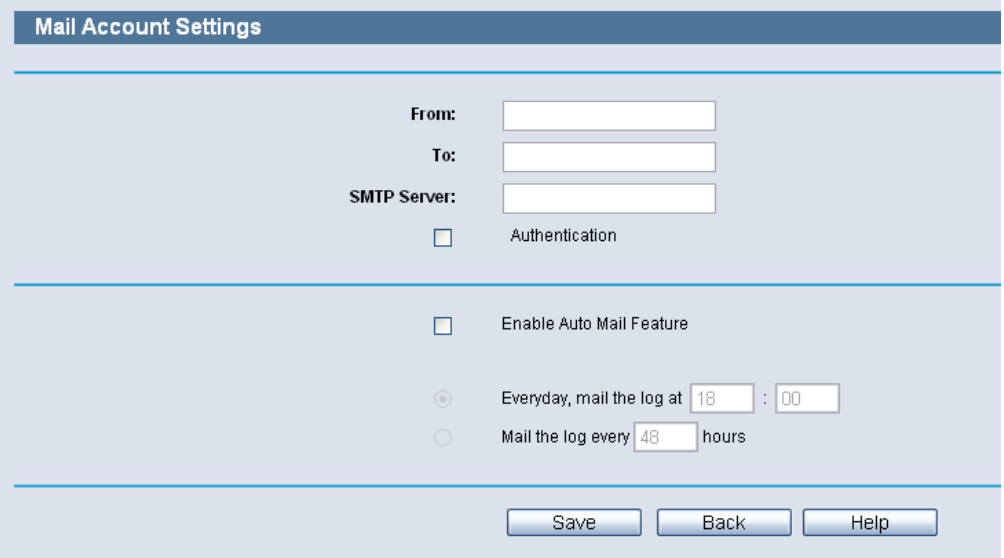
Choose menu "System Tools->System Log", you can view the logs of the Router.

Figure 102: System Log


System Log
Auto Mail Feature: Disabled
Mail Settings
Log Type: All
Log Level: ALL
Log is Empty.
Time = 2000-01-01 19:42:04 70925s
H-Ver = SMCWGBR14-N2 A1 : S-Ver = V1.0.0.0 Build 110524 Rel.36350n
L = 192.168.2.1 : M = 255.255.255.0
W1 = STATIC IP : W = 172.31.70.82 : M = 255.255.255.0 : G = 172.31.70.1
Refresh
Save Log
Mail Log
Clear Log

- **Auto Mail Feature** - Indicates whether auto mail feature is enabled or not.
- **Mail Settings** - Set the receiving and sending mailbox address, server address, validation information as well as the timetable for Auto Mail Feature, as shown in Figure 101.
- **Log Type** - By selecting the log type, only logs of this type will be shown.
- **Log Level** - By selecting the log level, only logs of this level will be shown.
- **Refresh** - Refresh the page to show the latest log list.
- **Save Log** - Click to save all the logs in a txt file.
- **Mail Log** - Click to send an email of current logs manually according to the address and validation information set in Mail Settings.
- **Clear Log -** All the logs will be deleted from the Router permanently, not just from the page.

Figure 103: Mail Account Settings



- **From** - Your mail box address. The Router would connect it to send logs.
- **To** - Recipient's address. The destination mailbox where the logs would be received.
- **SMTP Server** - Your smtp server. It corresponds with the mailbox filled in the From field. You can log on the relevant website for Help if you are not clear with the address.
- **Authentication** - Most SMTP Server requires Authentication. It is required by most mailboxes that need User Name and Password to log in.

NOTE: Only when you select Authentication, do you have to enter the User Name and Password in the following fields.

- **User Name** - Your mail account name filled in the From field. The part behind @ is excluded.
- **Password** - Your mail account password.
- **Confirm The Password** - Enter the password again to confirm.
- **Enable Auto Mail Feature** - Select it to mail logs automatically. You could mail the current logs either at a specified time everyday or by intervals, but only one could be the current effective rule. Enter the desired time or intervals in the corresponding field.

Click Save to keep your settings.

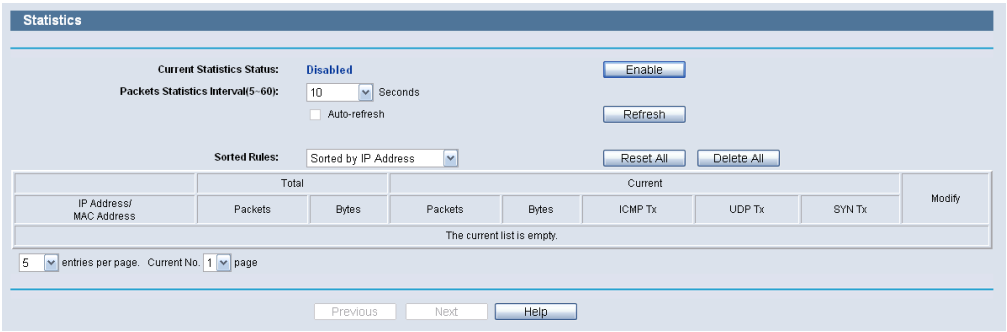
Click Back to return to the previous page.

Click the Next button to go to the next page, or click the Previous button return to the previous page.

STATISTICS

Choose menu "System Tools->Statistics", you can view the statistics of the Router, including total traffic and current traffic of the last Packets Statistic Interval.

Figure 104: Statistics



- **Current Statistics Status** - Enable or Disable. The default value is disabled. To enable, click the Enable button.
- **Packets Statistics Interval (5-60)** - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval indicates the time section of the packets statistic.

Select the Auto-refresh checkbox to refresh automatically.

Click the Refresh button to refresh immediately.

- **Sorted Rules** - Select a rule from the pull-down list to display the corresponding statistics..

Click Reset All to reset the values of all the entries to zero.

Click Delete All to delete all entries in the table.

Table 3: Statistics Table

IP/MAC Address		The IP/MAC Address displayed with statistics
Total	Packets	The total amount of packets received and transmitted by the Router.
	Bytes	The total amount of bytes received and transmitted by the Router
Current	Packets	The total amount of packets received and transmitted in the last Packets Statistic interval seconds.

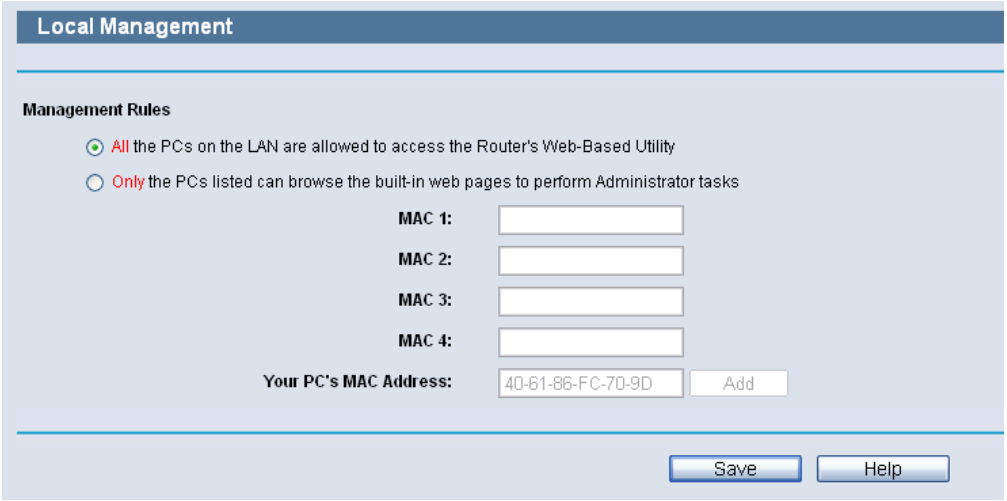
Table 3: Statistics Table (Continued)

Bytes	The total amount of bytes received and transmitted in the last Packets Statistic interval seconds.
ICMP Tx	The total amount of the ICMP packets transmitted to WAN in the last Packets Statistic interval seconds.
UDP Tx	The total amount of the UDP packets transmitted to WAN in the last Packets Statistic interval seconds.
TCP SYN Tx	The total amount of the TCP SYN packets transmitted to WAN in the last Packets Statistic interval seconds.

LOCAL MANAGEMENT

Choose menu "Security->Local Management", you can configure the management rule in the screen as shown in the following figure. The management feature allows you to deny computers in LAN from accessing the Router.

Figure 105: Local Management



By default, the radio button "All the PCs on the LAN are allowed to access the Router's Web-Based Utility" is checked. If you want to allow PCs with specific MAC Addresses to access the Setup page of the Router's Web-Based Utility locally from inside the network, check the radio button "Only the PCs listed can browse the built-in web pages to perform Administrator tasks", and then enter each MAC Address in a separate field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). Only the PCs with MAC address listed can use the password to browse the built-in web pages to perform Administrator tasks while all the others will be blocked.

After click the Add button, your PC's MAC Address will be placed in the list above.

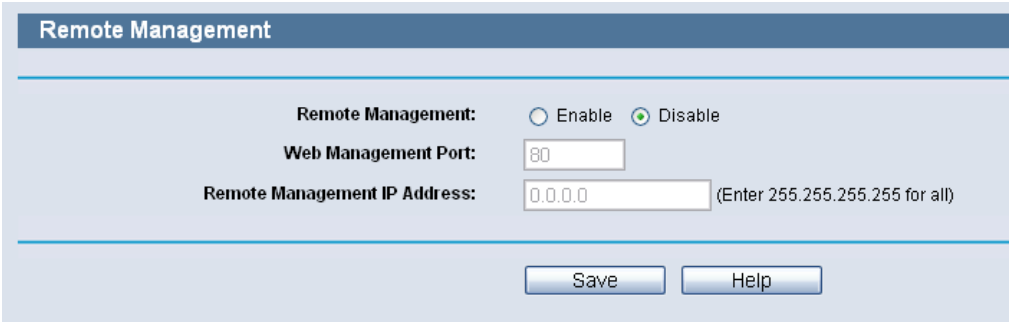
Click the Save button to save your settings.

NOTE: If your PC is blocked but you want to access the Router again, use a pin to press and hold the Reset Button (hole) on the back panel for about 5 seconds to reset the Router's factory defaults on the Router's Web-Based Utility.

REMOTE MANAGEMENT

Choose menu "Security->Remote Management", you can configure the Remote Management function in the screen as shown in the following figure. This feature allows you to manage your Router from a remote location via the Internet.

Figure 106: Remote Management



- **Web Management Port** - Web browser access normally uses the standard HTTP service port 80. This Router's default remote management web port number is 80. For greater security, you can change the remote management web port to a custom port by entering that number in the box provided. Choose a number between 1 and 65534 but do not use the number of any common service port.

- **Remote Management IP Address** - This is the current address you will use when accessing your Router from the Internet. This function is disabled when the IP address is set to the default value of 0.0.0.0. To enable this function change 0.0.0.0 to a valid IP address. If set to 255.255.255.255, then all the hosts can access the Router from internet.

NOTE: To access the Router, you should type your Router's WAN IP address into your browser's address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For example, if your Router's WAN address is 202.96.12.8, and the port number used is 8080, please enter http://202.96.12.8:8080 in your browser. Later, you may be asked for the Router's password. After successfully entering the username and password, you will be able to access the Router's web-based utility.

NOTE: Be sure to change the Router's default password to a very secure password.

A FAQ

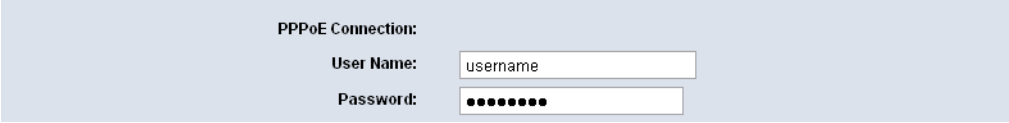
How do I configure the Router to access Internet by ADSL users?

1. First, configure the ADSL Modem configured in RFC1483 bridge model.

2. Connect the Ethernet cable from your ADSL Modem to the WAN port on the Router. The telephone cord plugs into the Line port of the ADSL Modem.

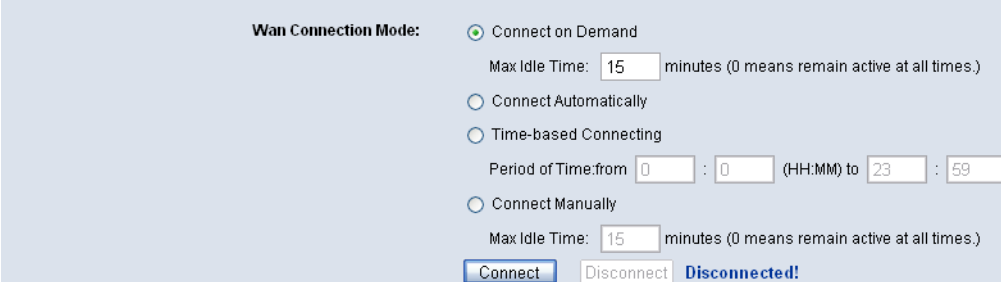
3. Login to the Router, click the “Network” menu on the left of your browser, and click "WAN" submenu. On the WAN page, select “PPPoE” for WAN Connection Type. Type user name in the “User Name” field and password in the “Password” field, finish by clicking “Connect”.

Figure 107: PPPoE Connection Type



4. If your ADSL lease is in “pay-according-time” mode, select “Connect on Demand” or “Connect Manually” for Internet connection mode. Type an appropriate number for “Max Idle Time” to avoid wasting paid time. Otherwise, you can select “Auto-connecting” for Internet connection mode.

Figure 108: PPPoE Connection Mode


Wan Connection Mode:
Connect on Demand
Max Idle Time: 15 minutes (0 means remain active at all times.)
Connect Automatically
Time-based Connecting
Period of Time:from 0 : 0 (HH:MM) to 23 : 59
Connect Manually
Max Idle Time: 15 minutes (0 means remain active at all times.)
Connect
Disconnect
Disconnected!

NOTE: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.

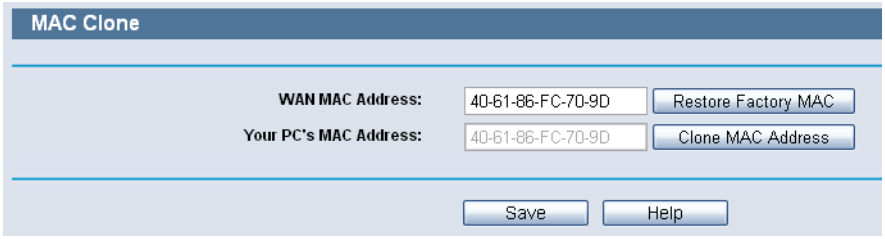
NOTE: If you are a Cable user, please configure the Router following the above steps.

How do I configure the Router to access Internet by Ethernet users?

1. Login to the Router, click the “Network” menu on the left of your browser, and click "WAN" submenu. On the WAN page, select “Dynamic IP” for "WAN Connection Type", finish by clicking “Save”.

2. Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable/DSL Modem during installation. If your ISP requires MAC register, login to the Router and click the "Network" menu link on the left of your browser, and then click "MAC Clone" submenu link. On the "MAC Clone" page, if your PC’s MAC address is proper MAC address, click the "Clone MAC Address" button and your PC’s MAC address will fill in the "WAN MAC Address" field. Or else, type the MAC Address into the "WAN MAC Address" field. The format for the MAC Address is XX-XX-XX-XX-XX-XX. Then click the "Save" button. It will take effect after rebooting.

Figure 109: MAC Clone



I want to use Netmeeting, what do I need to do?

1. If you start Netmeeting as a host, you don’t need to do anything with the Router.

2. If you start as a response, you need to configure Virtual Server or DMZ Host and make sure the H323 ALG is enabled.

3. How to configure Virtual Server: Log in to the Router, click the “Special Application” menu on the left of your browser, and click "Virtual Servers" submenu. On the "Virtual Servers" page, Click the Add New button. Then on the “Add or Modify a Virtual Server Entry” page, enter “1720” for the “Service Port” blank, and your IP address for the “IP Address” blank, taking 192.168.2.169 for an example, remember to Enable and Save.

Figure 110: Virtual Servers

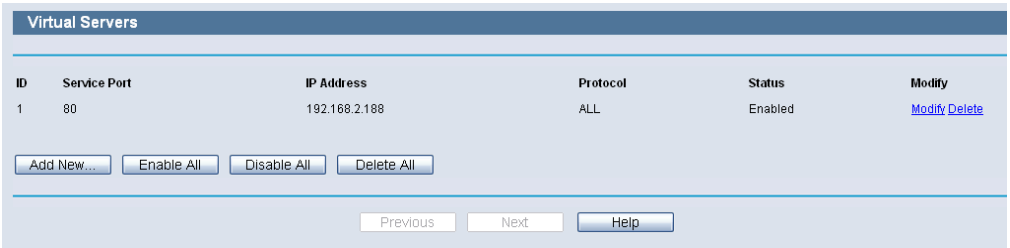
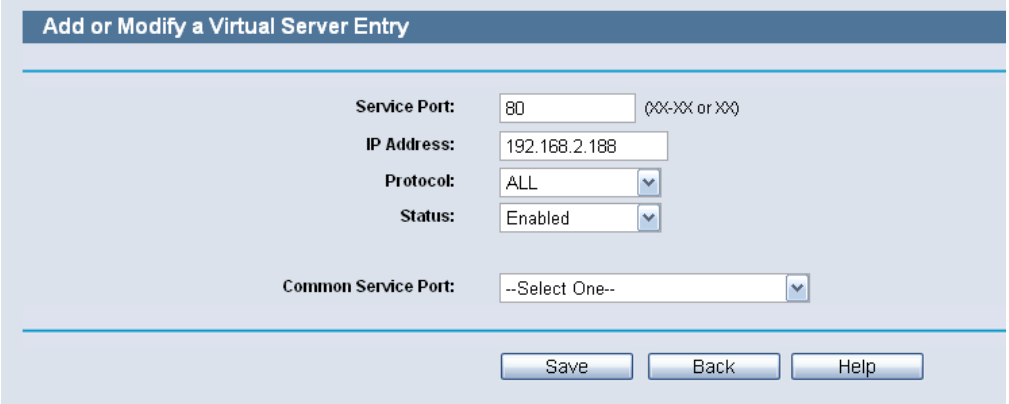


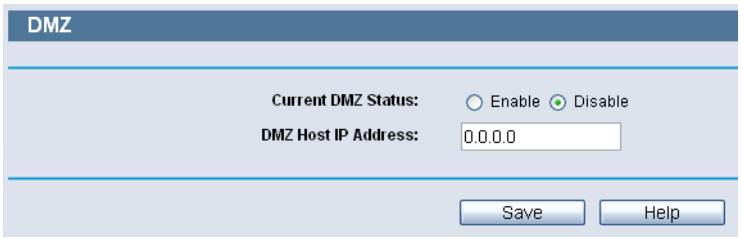
Figure 111: Virtual Servers



NOTE: Your opposite side should call your WAN IP, which is displayed on the "Status" page.

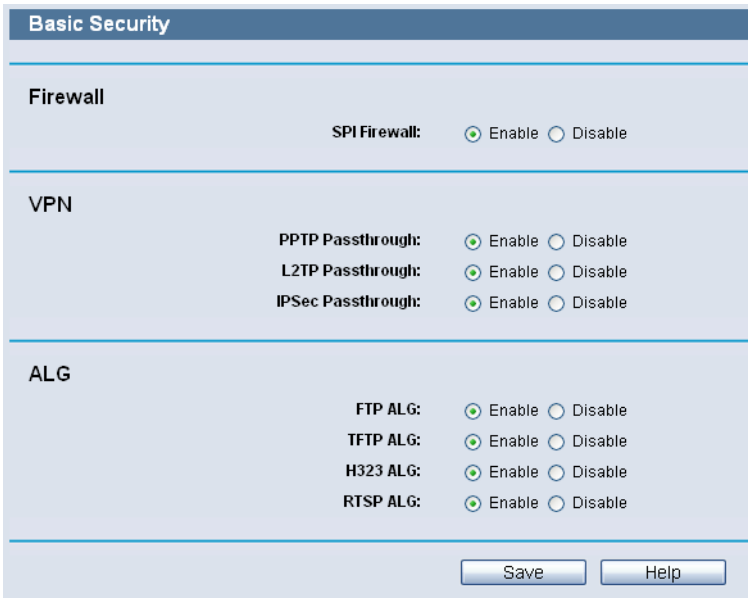
4. How to enable DMZ Host: Log in to the Router, click the "Special Application" menu on the left of your browser, and click "DMZ" submenu. On the "DMZ" page, click Enable radio button and type your IP address into the "DMZ Host IP Address" field, using 192.168.2.169 as an example, remember to click the Save button.

Figure 112: DMZ



5. How to enable H323 ALG: Log in to the Router, click the "Security" menu on the left of your browser, and click "Basic Security" submenu. On the "Basic Security" page, check the Enable radio button next to H323 ALG. Remember to click the Save button.

Figure 113: Basic Security

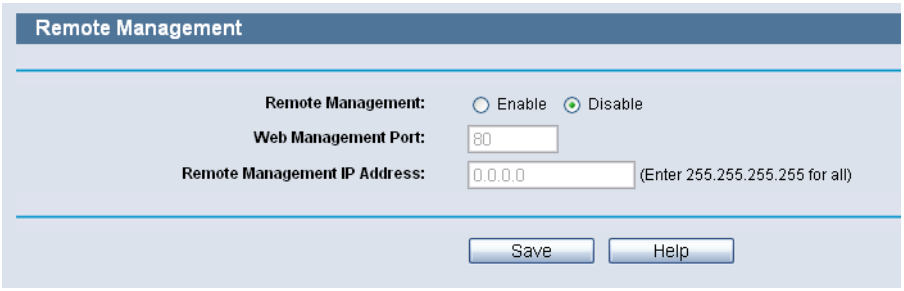


I want to build a WEB Server on the LAN, what should I do?

1. Because the WEB Server port 80 will interfere with the WEB management port 80 on the Router, you must change the WEB management port number to avoid interference.

2. To change the WEB management port number: Log in to the Router, click the "Security" menu on the left of your browser, and click "Remote Management" submenu. On the "Remote Management" page, type a port number except 80, such as 88, into the "Web Management Port" field. Click Save and reboot the Router.

Figure 114: Remote Management



NOTE: If the above configuration takes effect, to configure to the Router by typing http://192.168.2.1:88 (the Router's LAN IP address: Web Management Port) in the address field of the Web browser.

3. Log in to the Router, click the “Special Application” menu on the left of your browser, and click the "Virtual Servers" submenu. On the "Virtual Servers" page, Click the Add New button, then on the “Add or Modify a Virtual Server” page, enter “80” into the blank next to the “Service Port”, and your IP address next to the “IP Address”, assuming 192.168.2.188 for an example, remember to Enable and Save.

Figure 115: Virtual Servers

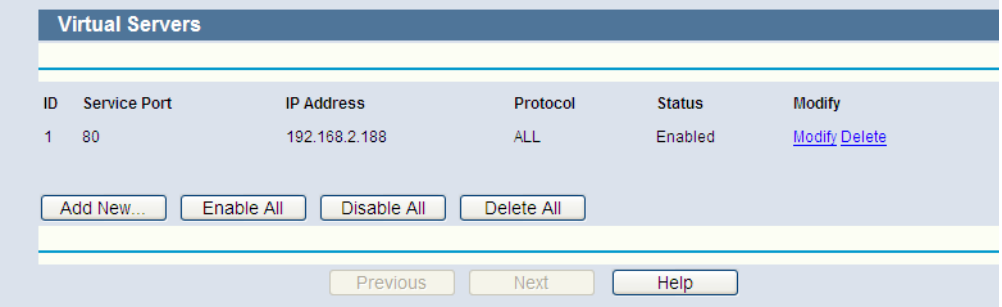
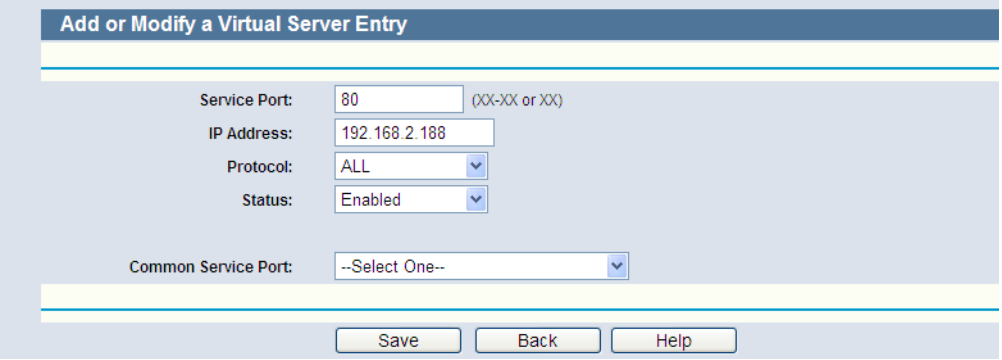


Figure 116: Add or Modify a Virtual Server Entry



The wireless stations cannot connect to the Router.

1. Make sure the "Wireless Router Radio" is enabled.

2. Make sure that the wireless stations' SSID accord with the Router's SSID.

3. Make sure the wireless stations have right KEY for encryption when the Router is encrypted.

4. If the wireless connection is ready, but you can’t access the Router, check the IP Address of your wireless stations.

B CONFIGURING THE PCS

In this section, we'll introduce how to install and configure the TCP/IP correctly in Windows XP. First make sure your Ethernet Adapter is working, refer to the adapter's manual if needed.

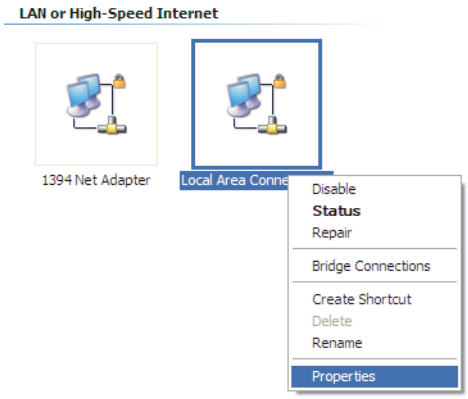
1. Install TCP/IP component

   a. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.

   b. Click the Network and Internet Connections icon, and then click on the Network Connections tab in the appearing window.

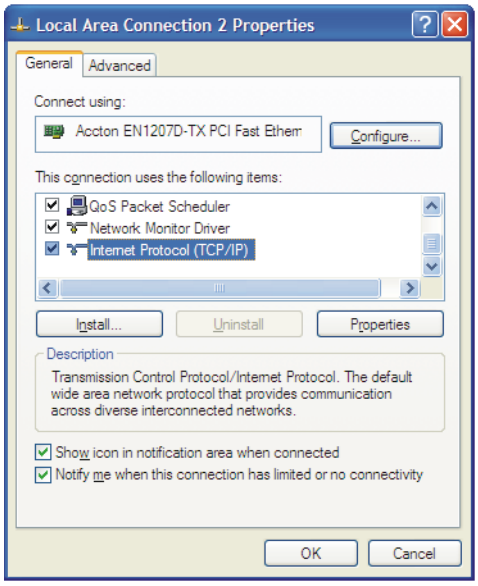
   c. Right click the icon that showed below, select Properties on the prompt page.

Figure 117: Internet Connection



   d. In the prompt page that showed below, double click on the Internet Protocol (TCP/IP).

Figure 118: Select TCP/IP



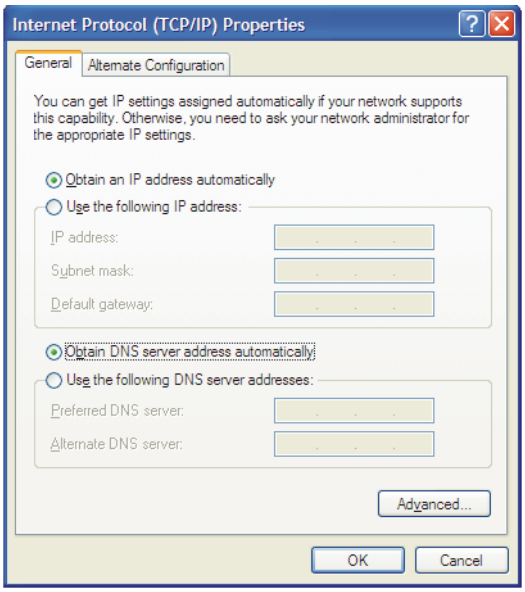
1.5 The following TCP/IP Properties window will display and the IP Address tab is open on this window by default.

Now you have two ways to configure the TCP/IP protocol below:

Setting IP address automatically

Select Obtain an IP address automatically, Choose Obtain DNS server automatically, as shown in the Figure below:

Figure 119: Obtain an IP address automatically


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Setting IP address manually

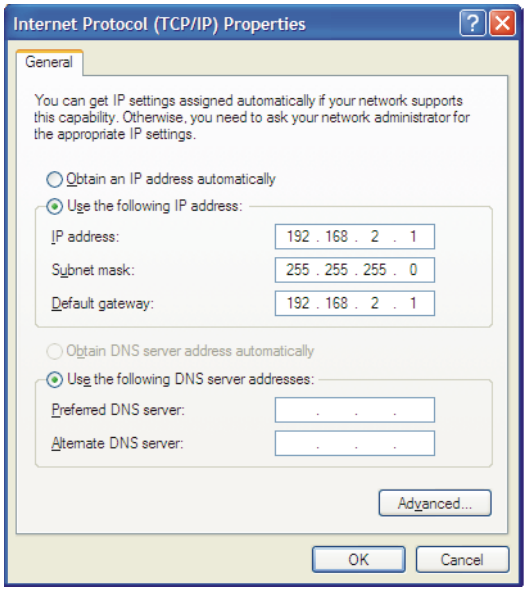
1. Select Use the following IP address radio button. And the following items available

2. If the Router's LAN IP address is 192.168.2.1, type IP address is 192.168.2.x (x is from 2 to 254), and Subnet mask is 255.255.255.0.

3. Type the Router's LAN IP address (the default IP is 192.168.2.1) into the Default gateway field.

4. Select Use the following DNS server addresses radio button. In the Preferred DNS Server field you can type the DNS server IP address, which has been provided by your ISP.

Figure 120: Use the Following IP


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 2 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 2 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

C HARDWARE SPECIFICATIONS

STANDARDS	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T 802.11b 802.11g 802.11n
PROTOCOL	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
NUMBER OF PORTS	1 10/100/1000 Mbps Auto-Negotiation WAN RJ-45 port 4 10/100/1000 Mbps Auto-Negotiation LAN RJ-45 ports supporting Auto MDI/MDIX 1 USB 2.0 port
CABLING TYPE	10BASE-T: UTP Category 3, 4, 5 cable (maximum 100 m) EIA/TIA-568 100 STP (maximum 100 m) 100BASE-TX: UTP Category 5, 5e cable (maximum 100 m) EIA/TIA-568 100 STP (maximum 100 m) 1000BASE-TX: UTP Category 5e, 6 cable (maximum 100 m) EIA/TIA-568 100 STP (maximum 100 m)
LED INDICATORS	Power, System, WLAN, WAN, LAN (1-4), USB, WPS
FREQUENCY BAND	2.4 ~ 2.4835 GHz
RADIO DATA RATE	11b: 11/5.5/2/1M (Automatic) 11g: 54/48/36/24/18/12/9/6M (Automatic) 11n: up to 300 Mbps (Automatic)
CHANNELS	13
FREQUENCY EXPANSION	DSSS (Direct Sequence Spread Spectrum)

MODULATION	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
SECURITY	WEP/WPA/WPA2/WPA2-PSK/WPA-PSK
SENSITIVITY @PER	270M: -68dBm@10% PER; 130M: -68dBm@10% PER 108M: -68dBm@10% PER; 54M: -68dBm@10% PER 11M: -85dBm@8% PER; 6M: -88dBm@10% PER 1M: -90dBm@8% PER
RF POWER	20dBm (max EIRP)
ANTENNA GAIN	3dBi*3
TEMPERATURE	Operating: 0 °C to 40 °C (32 to 104 °F) Storage: -40 °C to 70 °C (-40 to 158 °F)
HUMIDITY	Operating: 10% to 90% (non-condensing) Storge: 5%-90% (non-condensing)

GLOSSARY

IEEE 802.11B A wireless standard that supports wireless communications in the 2.4 GHz band using Direct Sequence Spread Spectrum (DSSS). The standard provides for data rates of 1, 2, 5.5, and 11 Mbps.

IEEE 802.11G A wireless standard that supports wireless communications in the 2.4 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard provides for data rates of 6, 9, 12, 18, 24, 36, 48, 54 Mbps. IEEE 802.11g is also backward compatible with IEEE 802.11b.

IEEE 802.11N A wireless standard that supports wireless communications in the 2.4 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard provides for data rates of 27, 54, 81, 108, 162, 216, 243, 270, 300 Mbps. IEEE 802.11n is also backward compatible with IEEE 802.11b/g.

DDNS (DYNAMIC DOMAIN NAME SYSTEM) The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.

DHCP Dynamic Host Configuration Protocol: Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

DMZ (DEMILITARIZED ZONE) A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.

DNS (DOMAIN NAME SYSTEM) An Internet Service that translates the names of websites into IP addresses.

DOMAIN NAME A descriptive name for an address or group of addresses on the Internet.

DSL (DIGITAL SUBSCRIBER LINE) A technology that allows data to be sent or received over existing traditional phone lines.

ISP (INTERNET SERVICE PROVIDER) A company that provides access to the Internet.

MTU (MAXIMUM TRANSMISSION UNIT) The size in bytes of the largest packet that can be transmitted.

NAT (NETWORK ADDRESS TRANSLATION) NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

PPPOE (POINT TO POINT PROTOCOL OVER ETHERNET) PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

SSID A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.

WEP (WIRED EQUIVALENT PRIVACY) A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.

WI-FI A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.

WLAN (WIRELESS LOCAL AREA NETWORK) A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.

Headquarters & Sub-Sahara Africa Office

No. 1, Creation Rd. III
Hsinchu Science Park
Taiwan 30077
Tel: +886 3 5770270
Fax: +886 3 5780764

Asia-Pacific Office

1 Coleman Street
#07-09, The Adelphi
Singapore 179803
Tel: +65-63387667
Fax: +65-63387767

Europe & N. Africa Office

C/Fructuós Gelabert 6-8, 2º, 2ª
Edificio Conata II
08970 Sant Joan Despí
Barcelona, Spain
Tel: +34 93 477 4920

Middle East Office

Office No. 416, Le Solarium Bldg
Dubai Silicon Oasis
Dubai, U.A.E.
Tel: +971-4-3564800
Fax:+971-4-3564801

North America Office

20 Mason
Irvine CA 92618 U.S.A.
Tel: +1 (949) 679-8000

SMC NETWORKS TECHNICAL SUPPORT

From Singapore in English and 中文 (Mon.-Fri. 9 AM to 5 PM)
Tel: +65-63387667, Ext. 4

From the United Arab Emirates in English (Sun.-Thu. 9 AM to 6 PM)
Tel: +971 800 222866/+971 4 3564810

From U.S.A. and Canada (24 hours a day, 7 days a week)
Tel: +1 (800) SMC-4-YOU/+1 (949) 679-8000 Fax: +1 (949) 679-1481

English: Technical Support information available at www.smc.com

English: (for Asia-Pacific): Technical Support information at www.smc-asia.com

English: (for Middle East): Technical Support information at muneer@smc-asia.com

Deutsch: Technischer Support und weitere Information unter www.smc.com

Español: En www.smc.com Ud. podrá encontrar la información relativa a servicios de soporte técnico

Français: Informations Support Technique sur www.smc.com

Português: Informações sobre Suporte Técnico em www.smc.com

Italiano: Le informazioni di supporto tecnico sono disponibili su www.smc.com

Svenska: Information om Teknisk Support finns tillgängligt på www.smc.com

Nederlands: Technische ondersteuningsinformatie beschikbaar op www.smc.com

Polski: Informacje o wsparciu technicznym sa dostepne na www.smc.com

Čeština: Technicka podpora je dostupna na www.smc.com

Magyar: Műszaki tamogat informacio elerhető -on www.smc.com

简体中文：技术支持讯息可通过www.smc-prc.com查询

繁體中文：產品技術支援與服務請上 www.smcnetworks.com.tw

ไทย: สามารถหาข้อมูลทางด้านเทคนิคได้ที่ www.smc-asia.com

한국어: 기술지원관련 정보는 www.smcnetworks.co.kr 을 참고하시기 바랍니다

INTERNET
E-mail address: www.smc.com→ Support→ By email
Driver updates: www.smc.com→ Support→ Downloads

SMCWGBR14-N2